DevConnect Program

Application Notes for Configuring Avaya IP Office Server Edition R12.0 with Avaya Session Border Controller R10.2 to support Swisscom Enterprise SIP Trunk Service 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between the Swisscom Enterprise SIP Trunk Service and Avaya IP Office Server Edition R12.0 with Avaya Session Border Controller R10.2.

The Swisscom Enterprise SIP Trunk provides PSTN access via a SIP trunk connected to the Swisscom Enterprise SIP Voice Over Internet Protocol (VoIP) network as an alternative to legacy Analog or Digital trunks. Swisscom is a member of the Avaya DevConnect Service Provider program.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Swisscom Enterprise SIP Trunk service and Avaya IP Office Server Edition with Avaya Session Border Controller (Avaya SBC).

Avaya IP Office is a versatile communications solution that combines the reliability and ease of a traditional telephony system with the applications and advantages of an IP telephony solution. This converged communications solution can help businesses reduce costs, increase productivity, and improve customer service.

The Avaya Session Border Controller (Avaya SBC) is the point of connection between Avaya IP Office and Swisscom Enterprise SIP Trunk service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signalling for interoperability.

Swisscom Enterprise SIP Trunk service provides PSTN access via a SIP trunk connected to the Swisscom network as an alternative to legacy Analog or Digital trunks. This approach generally results in lower cost for customers

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office Server Edition and Avaya SBC to connect to the Swisscom Enterprise SIP Trunk. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For security, TLS and SRTP was used internally to the enterprise between Avaya products.

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability the following features and functionality were exercised during the interoperability compliance test:

- Incoming PSTN calls to various phone types including H.323, SIP, Digital and Analog telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, Digital, and Analog telephones at the enterprise.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to the Service Provider.
- Incoming and Outgoing PSTN calls to/from Avaya Workplace Client for Windows soft phone.
- Calls using the G.711A codec.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using G.711 pass-through transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- Various call types including local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, call mute, transfer, and conference.
- Off-net call forwarding and mobile twinning.

2.2. Test Results

Interoperability testing of the test configuration was completed with successful results for Swisscom's SIP Trunk service with the following observations:

- During T.38 fax testing, it was observed that when Swisscom sent a reINVITE to negotiate to T.38 fax calls, IP Office responded with a 200 OK with 2 x media lines in the SDP. The first media line had an attribute value of "inactive" which made the second media line active. However, the Avaya SBC was removing the SDP from the 200 OK and inserting a Warning Header " Internal Error 5" into the 200 OK Message header . The Avaya SBC would then forward this 200 OK without SDP to Swisscom and Swisscom would respond to the 200 OK from Avaya SBC with a BYE and the call was terminated. This issue is currently under investigation with Avaya. Therefore, T.38 fax is not currently supported on the Swisscom Enterprise SIP platform.
- The Privacy Header as required by Swisscom is not included in the SIP INVITE for outbound calls with Calling Line Identity Restriction (CLIR) when using an IP Office short code (*67 was used in the test configuration). As a workaround, the anonymous button can be enabled on the SIP tab in **Section 5.7** to restrict CLIR and include a Privacy Header as required by Swisscom.
- No inbound toll-free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.

- Access to Emergency Services was not tested as no test call had been booked by the Service Provider with the Emergency Services Operator

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

For technical support on Swisscom products please contact the Swisscom support team:
Email: ent.incident-voice@swisscom.com.

3. Reference Configuration

Figure 1 below illustrates the test configuration. The test configuration shows an enterprise site connected to the Swisscom Enterprise SIP Trunk. Located at the enterprise site is an Avaya IP Office Server Edition, an Avaya IP Office 500 V2 as an Expansion and an Avaya Session Border Controller. Endpoints include Avaya 1600 Series IP Telephones (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware), Avaya 1140e SIP Telephones, Avaya 1400 Series Digital Deskphones, Analog Telephone and a fax machine. The site also has a Windows 7 PC running Avaya IP Office Manager to configure the Avaya IP Office as well as Avaya Workplace Client for Windows for softphone testing.

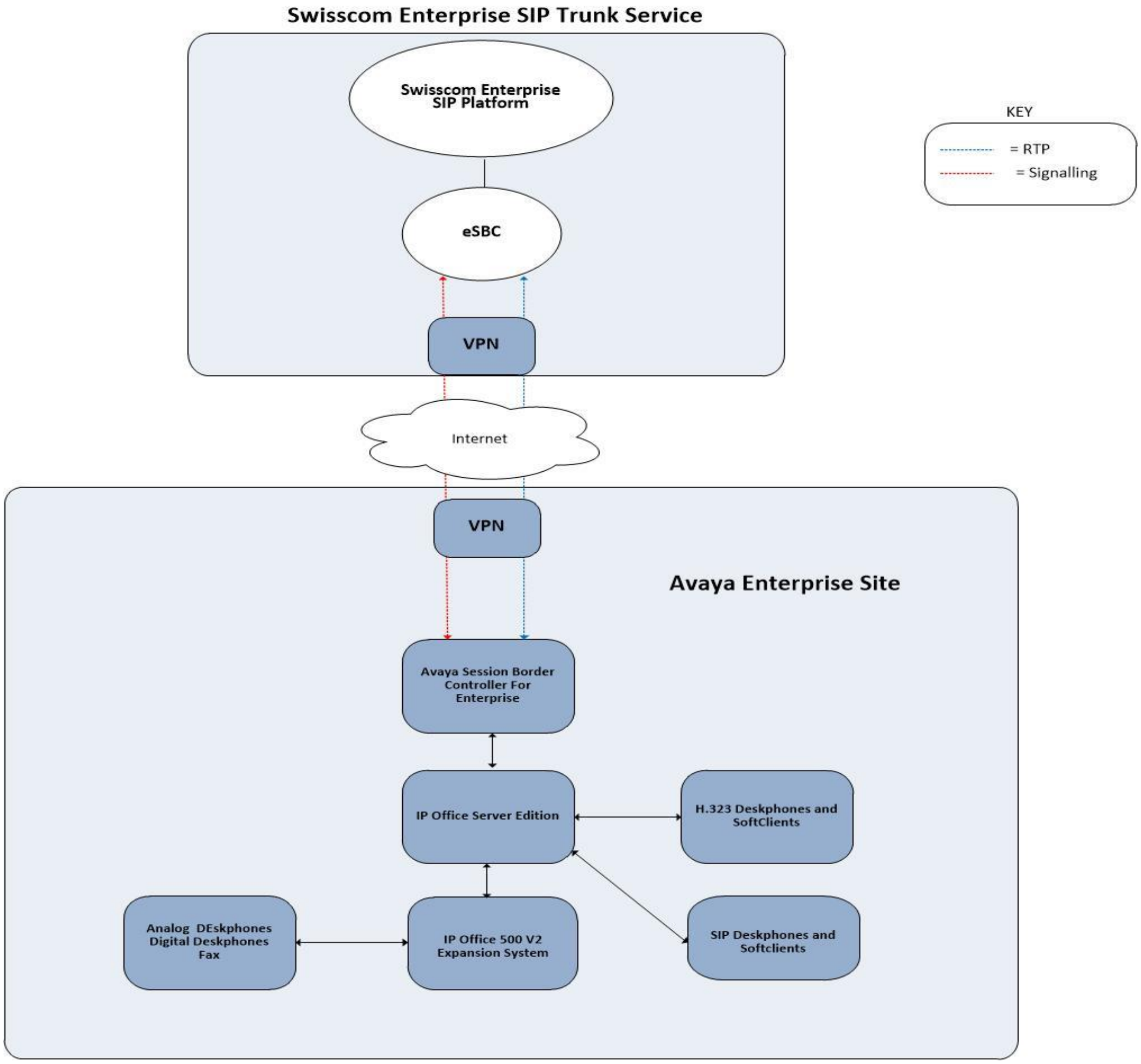

Swisscom Enterprise SIP Trunk Service
Swisscom Enterprise SIP Platform
KEY
= RTP
= Signalling
eSBC
VPN
Internet
VPN
Avaya Enterprise Site
Avaya Session Border Controller For Enterprise
IP Office Server Edition
H.323 Deskphones and SoftClients
Analog DEskphones Digital Deskphones Fax
IP Office 500 V2 Expansion System
SIP Deskphones and Softclients

Figure 1: Test setup Swisscom Enterprise SIP Trunk to simulated Avaya Enterprise

4. Equipment and Software Validated

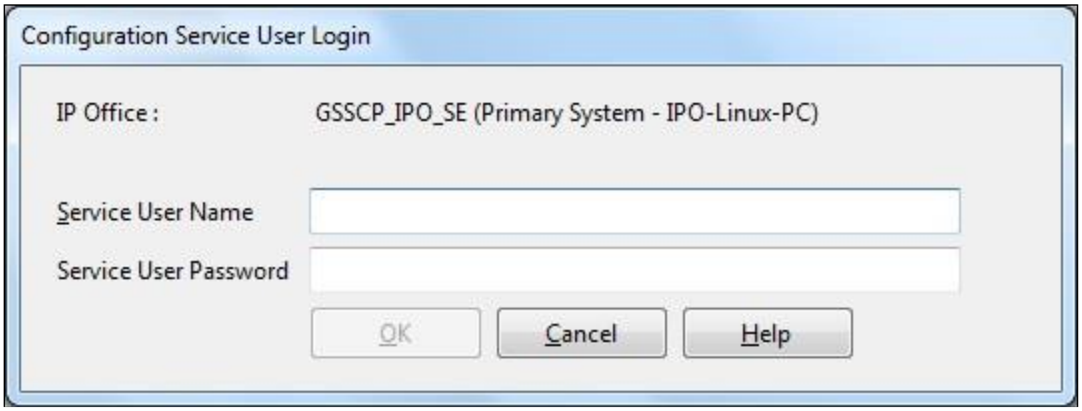
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	Version 12.0.0.0.0 build 56
Avaya IP Office 500 V2	Version 12.0.0.0.0 build 56
Avaya Voicemail Pro Client	Version 12.0.0.26
Avaya IP Office Manager	Version 12.0.0.0.0 build 56
Avaya Session Border Controller	10.2.0.1-89-24401
Avaya 1608 Phone (H.323)	1.3.12
Avaya 9611G Series Phone (H.323)	6.8.3
Avaya 9608 Series Phone (H.323)	6.8.3
Avaya J179 IP Phone (SIP)	4.0.10
Avaya Workplace for Windows (SIP)	3.36.0
Avaya 1140e (SIP)	FW: 04.04.30.00.bin
Avaya 1408 Digital Telephone	R48
Avaya 98390 Analogue Phone	N/A
Swisscom	
eSBC	Cisco IOS XE Software, Version 17.06.04
C-SBC	Oracle SCZ9.1.0
SESM	Ribbon 21.0.26

Note – Testing was performed with IP Office Server Edition with 500 V2 Expansion R12.0. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks, this includes T.38 fax.

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to the Swisscom SIP trunk. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials.

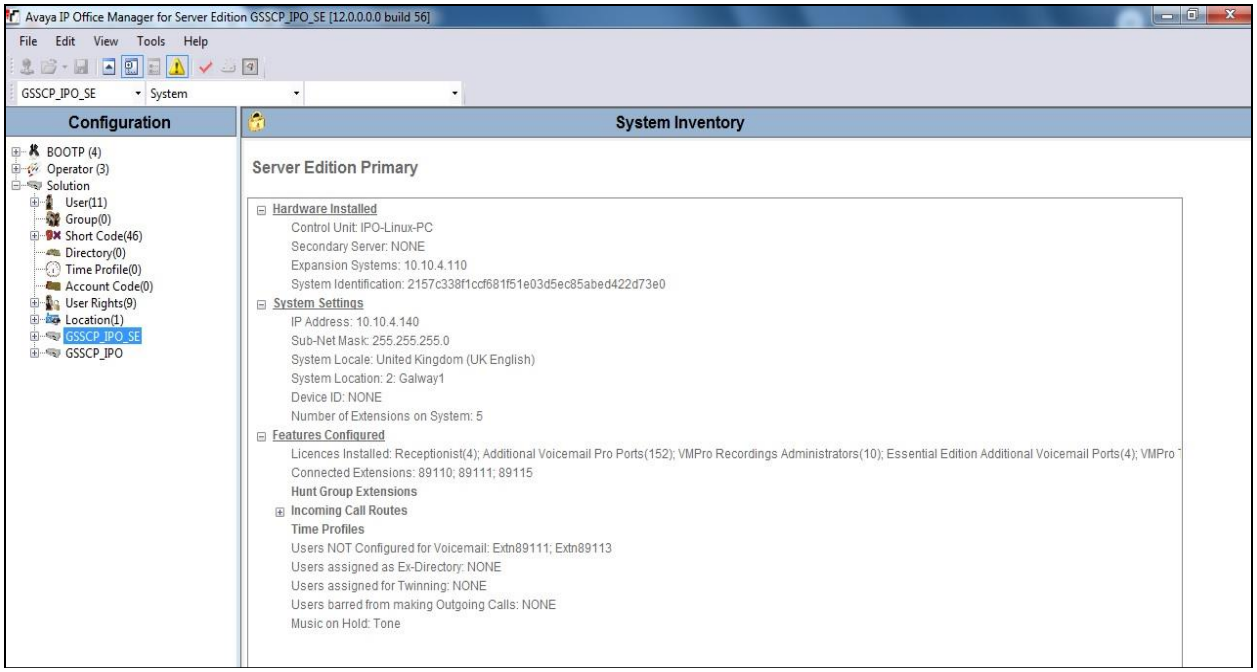


IP Office : GSSCP_IPO_SE (Primary System - IPO-Linux-PC)

Service User Name

Service User Password

A management window will appear similar to the one in the next section. All the Avaya IP Office configurable components are shown in the left pane known as the Navigation Pane. The pane on the right is the Details Pane. These panes will be referenced throughout the Avaya IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the Service Provider (such as twinning) is assumed to already be in place.



Server Edition Primary

Hardware Installed

- Control Unit: IPO-Linux-PC
- Secondary Server: NONE
- Expansion Systems: 10.10.4.110
- System Identification: 2157c338f1ccf681f51e03d5ec85abed422d73e0

System Settings

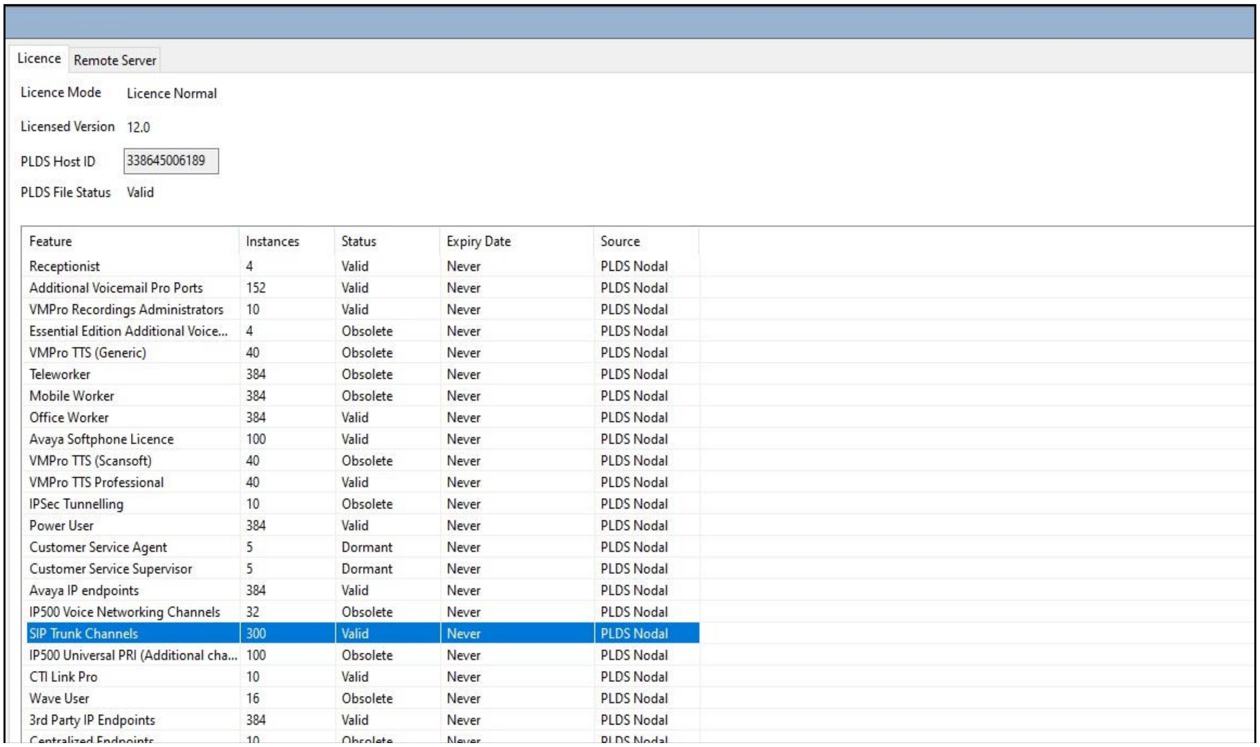
- IP Address: 10.10.4.140
- Sub-Net Mask: 255.255.255.0
- System Locale: United Kingdom (UK English)
- System Location: 2: Galway1
- Device ID: NONE
- Number of Extensions on System: 5

Features Configured

- Licences Installed: Receptionist(4); Additional Voicemail Pro Ports(152); VMPro Recordings Administrators(10); Essential Edition Additional Voicemail Ports(4); VMPro
- Connected Extensions: 89110; 89111; 89115
- Hunt Group Extensions
- Incoming Call Routes
- Time Profiles
- Users NOT Configured for Voicemail: Extn89111; Extn89113
- Users assigned as Ex-Directory: NONE
- Users assigned for Twinning: NONE
- Users barred from making Outgoing Calls: NONE
- Music on Hold: Tone

5.1. Verify System Capacity

Navigate to **License → SIP Trunk Channels** in the Navigation Pane. In the Details Pane, verify that the **License Status** is Valid and that the number of **Instances** is sufficient to support the number of SIP trunk channels provisioned by Swisscom.



Licence Mode Licence Normal

Licensed Version 12.0

PLDS Host ID 338645006189

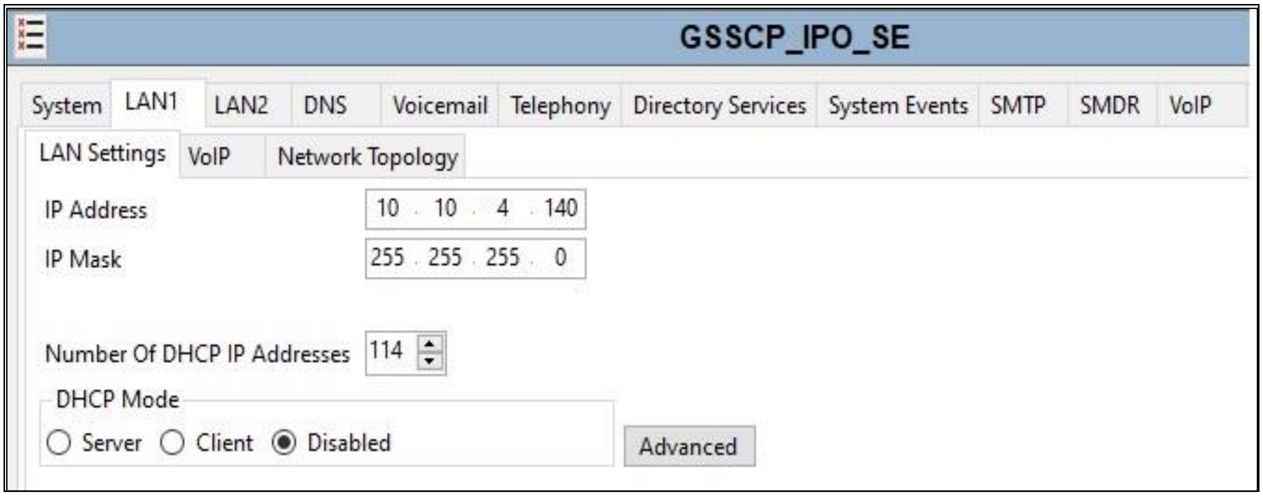
PLDS File Status Valid

Feature	Instances	Status	Expiry Date	Source
Receptionist	4	Valid	Never	PLDS Nodal
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal
VMPro Recordings Administrators	10	Valid	Never	PLDS Nodal
Essential Edition Additional Voice...	4	Obsolete	Never	PLDS Nodal
VMPro TTS (Generic)	40	Obsolete	Never	PLDS Nodal
Teleworker	384	Obsolete	Never	PLDS Nodal
Mobile Worker	384	Obsolete	Never	PLDS Nodal
Office Worker	384	Valid	Never	PLDS Nodal
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal
VMPro TTS (Scansoft)	40	Obsolete	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
IPSec Tunnelling	10	Obsolete	Never	PLDS Nodal
Power User	384	Valid	Never	PLDS Nodal
Customer Service Agent	5	Dormant	Never	PLDS Nodal
Customer Service Supervisor	5	Dormant	Never	PLDS Nodal
Avaya IP endpoints	384	Valid	Never	PLDS Nodal
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal
SIP Trunk Channels	300	Valid	Never	PLDS Nodal
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal
CTI Link Pro	10	Valid	Never	PLDS Nodal
Wave User	16	Obsolete	Never	PLDS Nodal
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal
Centralized Endpoints	10	Obsolete	Never	PLDS Nodal

5.2. LAN1 Settings

In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side). For the compliance test, the **LAN1** interface was used to the Avaya IP Office to the internal side of the Avaya SBC as these are on the same LAN, **LAN2** was not used.

To access the LAN1 settings, first navigate to **System → GSSCP_IPO_SE** in the Navigation Pane where GSSCP_IPO_SE is the name of the IP Office. Navigate to the **LAN1 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the private interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).

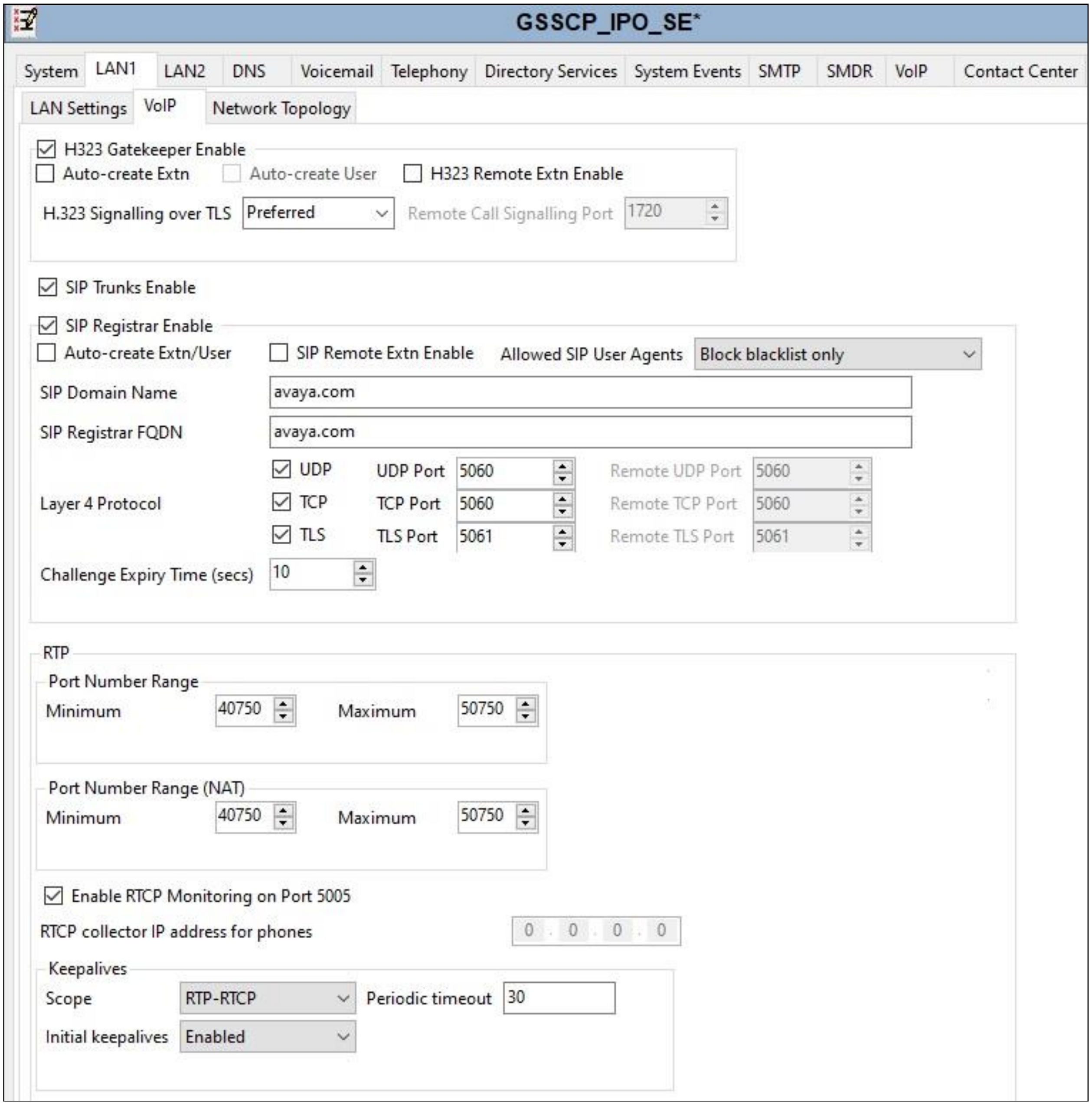


IP Address: 10 . 10 . 4 . 140
IP Mask: 255 . 255 . 255 . 0
Number Of DHCP IP Addresses: 114
DHCP Mode: ○ Server ○ Client ● Disabled

On the **VoIP** tab in the Details Pane, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol. Set **H.323 Signalling over TLS** to **Preferred** to allow IP Office endpoints to use TLS for signalling. Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. If SIP Endpoints are to be used such as the Avaya Communicator for Windows and the Avaya 1140e, the **SIP Registrar Enable** box must also be checked. The **Domain Name** has been set to the customer premises equipment domain "**avaya.com**.". If the **Domain Name** is left at the default blank setting, SIP registrations may use the IP Office LAN1 IP Address. All other parameters shown are default values.

The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Set **Scope** to **RTP-RTCP** and **Initial keepalives** to **Enabled** and **Periodic timeout** to **30**.

Avaya IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for both signalling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signalling. The specific values used for the compliance test are shown in the example below. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).



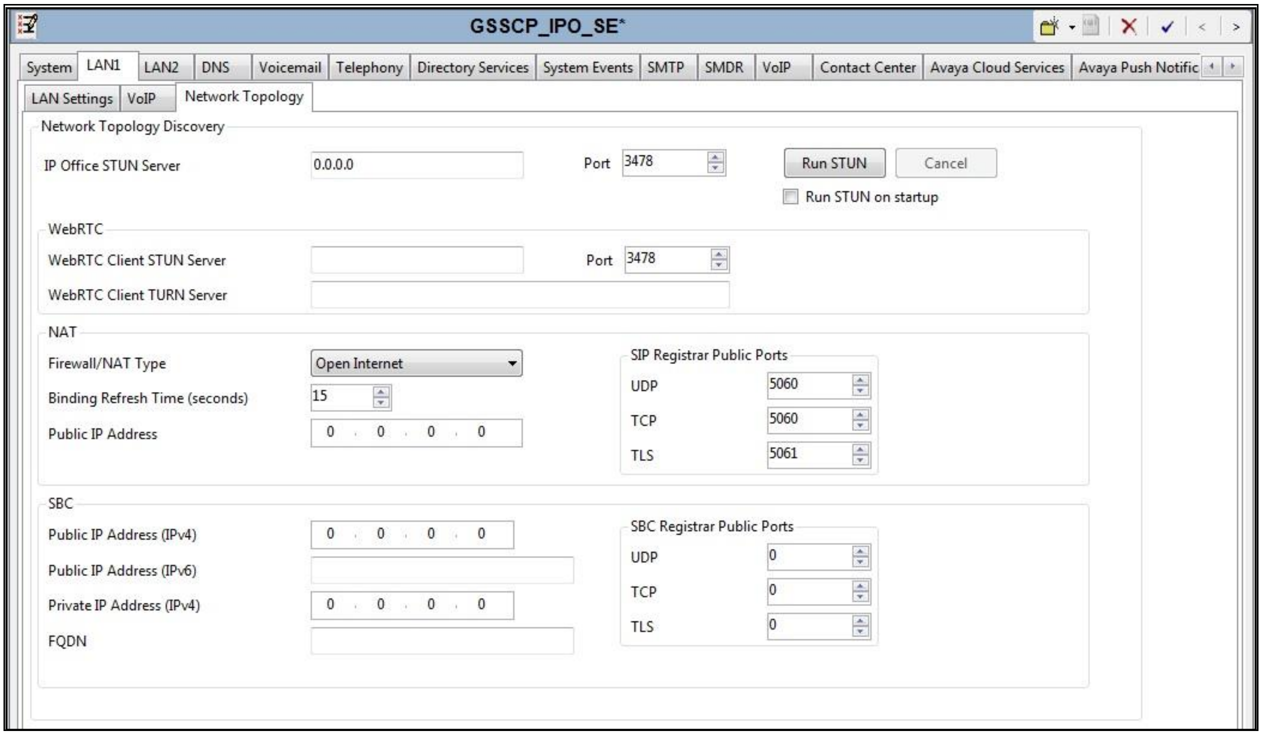
☑ H323 Gatekeeper Enable
☐ Auto-create Extn ☐ Auto-create User ☐ H323 Remote Extn Enable
H.323 Signalling over TLS: Preferred
Remote Call Signalling Port: 1720

☑ SIP Trunks Enable

☑ SIP Registrar Enable
☐ Auto-create Extn/User ☐ SIP Remote Extn Enable
Allowed SIP User Agents: Block blacklist only
SIP Domain Name: avaya.com
SIP Registrar FQDN: avaya.com
Layer 4 Protocol:
☑ UDP UDP Port: 5060 Remote UDP Port: 5060
☑ TCP TCP Port: 5060 Remote TCP Port: 5060
☑ TLS TLS Port: 5061 Remote TLS Port: 5061
Challenge Expiry Time (secs): 10

RTP
Port Number Range
Minimum: 40750 Maximum: 50750
Port Number Range (NAT)
Minimum: 40750 Maximum: 50750
☑ Enable RTCP Monitoring on Port 5005
RTCP collector IP address for phones: 0 . 0 . 0 . 0
Keepalives
Scope: RTP-RTCP Periodic timeout: 30
Initial keepalives: Enabled

On the **Network Topology** tab, set the **Firewall/NAT Type** from the pulldown menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used as NAT was not required for this configuration, therefore resulting in no requirement for a STUN server. The **Use Network Topology Info** in the **SIP Line** was set to **None** in **Section 5.6.2**. Set **Binding Refresh Time (seconds)** to **30**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider. Default values were used for all other parameters. On completion, click the **OK** button (not shown).



Network Topology Discovery

IP Office STUN Server: 0.0.0.0 Port: 3478

□ Run STUN on startup

WebRTC

WebRTC Client STUN Server: Port: 3478

WebRTC Client TURN Server:

NAT

Firewall/NAT Type: Open Internet

Binding Refresh Time (seconds): 15

Public IP Address: 0 . 0 . 0 . 0

SIP Registrar Public Ports

UDP: 5060

TCP: 5060

TLS: 5061

SBC

Public IP Address (IPv4): 0 . 0 . 0 . 0

Public IP Address (IPv6):

Private IP Address (IPv4): 0 . 0 . 0 . 0

FQDN:

SBC Registrar Public Ports

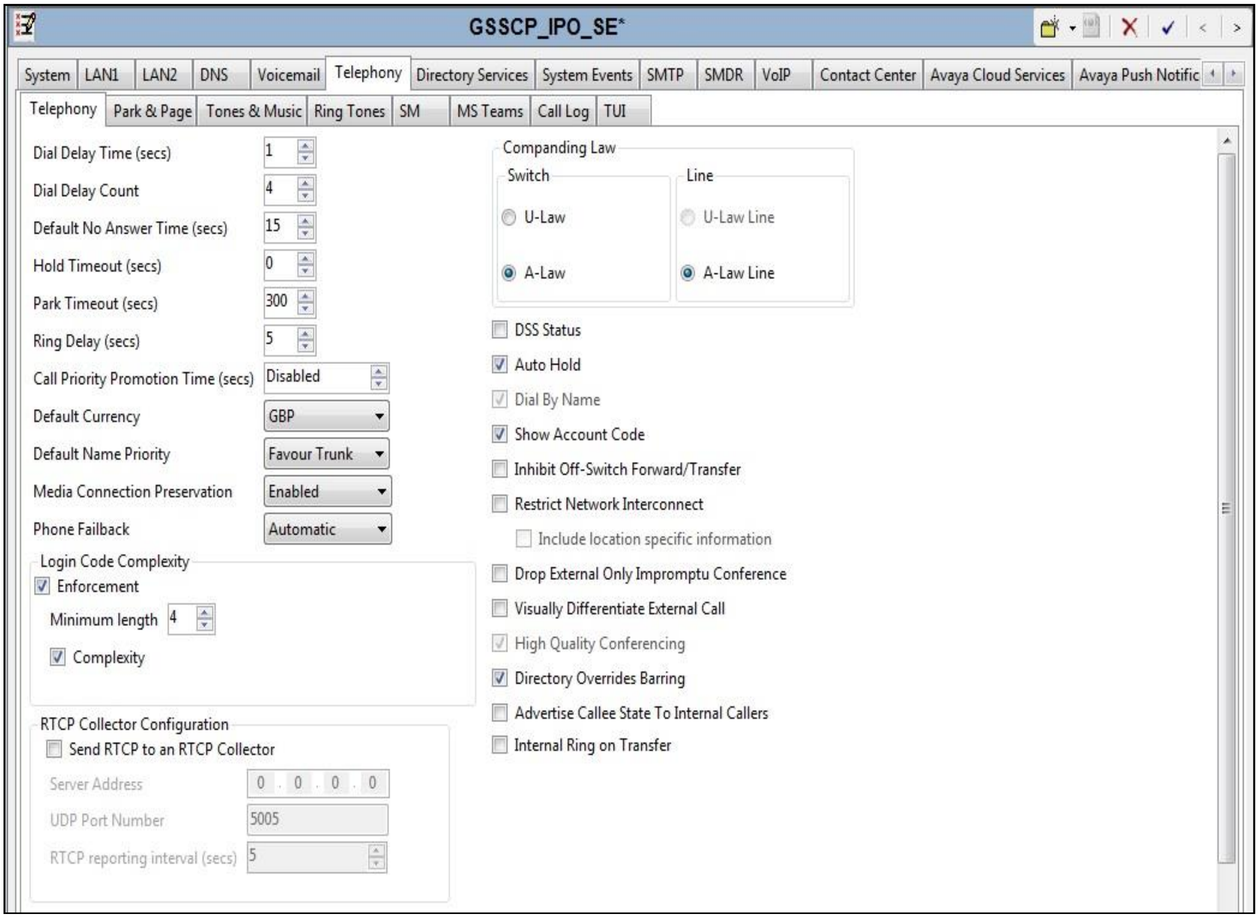
UDP: 0

TCP: 0

TLS: 0

5.3. System Telephony Settings

Navigate to the **Telephony → Telephony** tab on the Details Pane. Choose the **Companding Law** typical for the enterprise location. For Europe, **ALAW** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the Service Provider across the SIP trunk. On completion, click the **OK** button (not shown).



Dial Delay Time (secs) 1

Dial Delay Count 4

Default No Answer Time (secs) 15

Hold Timeout (secs) 0

Park Timeout (secs) 300

Ring Delay (secs) 5

Call Priority Promotion Time (secs) Disabled

Default Currency GBP

Default Name Priority Favour Trunk

Media Connection Preservation Enabled

Phone Failback Automatic

Login Code Complexity

☑ Enforcement

Minimum length 4

☑ Complexity

RTCP Collector Configuration

□ Send RTCP to an RTCP Collector

Server Address 0 . 0 . 0 . 0

UDP Port Number 5005

RTCP reporting interval (secs) 5

Companding Law

Switch: ○ U-Law ● A-Law

Line: ○ U-Law Line ● A-Law Line

□ DSS Status

☑ Auto Hold

☑ Dial By Name

☑ Show Account Code

□ Inhibit Off-Switch Forward/Transfer

□ Restrict Network Interconnect

□ Include location specific information

□ Drop External Only Impromptu Conference

□ Visually Differentiate External Call

☑ High Quality Conferencing

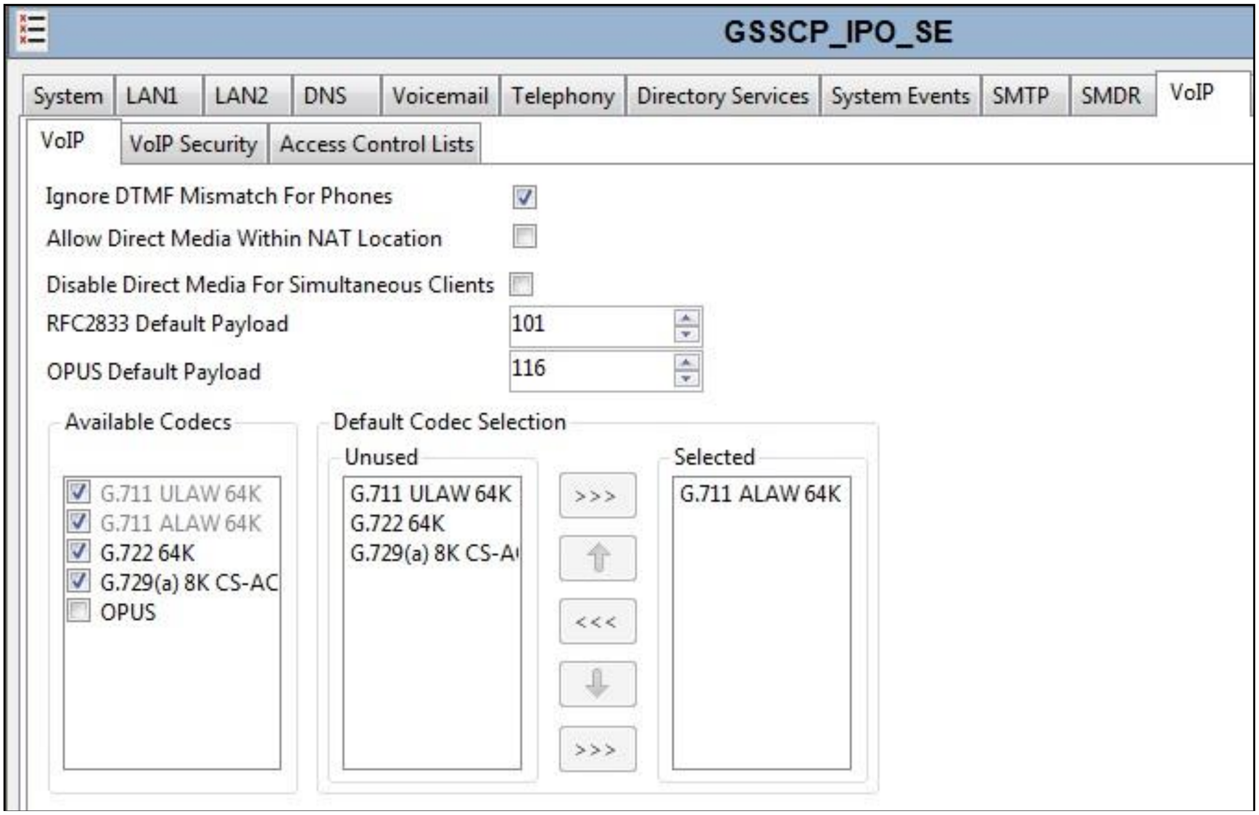
☑ Directory Overrides Barring

□ Advertise Callee State To Internal Callers

□ Internal Ring on Transfer

5.4. VoIP Settings

Navigate to the **VoIP** tab on the Details Pane. Check the available Codecs boxes as required. Note that **G.711 ULAW 64K** and **G.711 ALAW 64K** are greyed out and always available. Once available codecs are selected, they can be used or unused by using the horizontal arrows as required. Note that in test, **G.711 ALAW 64K** is set as the priority codec selection.



Ignore DTMF Mismatch For Phones ☑

Allow Direct Media Within NAT Location □

Disable Direct Media For Simultaneous Clients □

RFC2833 Default Payload 101

OPUS Default Payload 116

Available Codecs

- ☑ G.711 ULAW 64K
- ☑ G.711 ALAW 64K
- ☑ G.722 64K
- ☑ G.729(a) 8K CS-AC
- □ OPUS

Default Codec Selection

Unused

G.711 ULAW 64K
G.722 64K
G.729(a) 8K CS-A

Selected

G.711 ALAW 64K

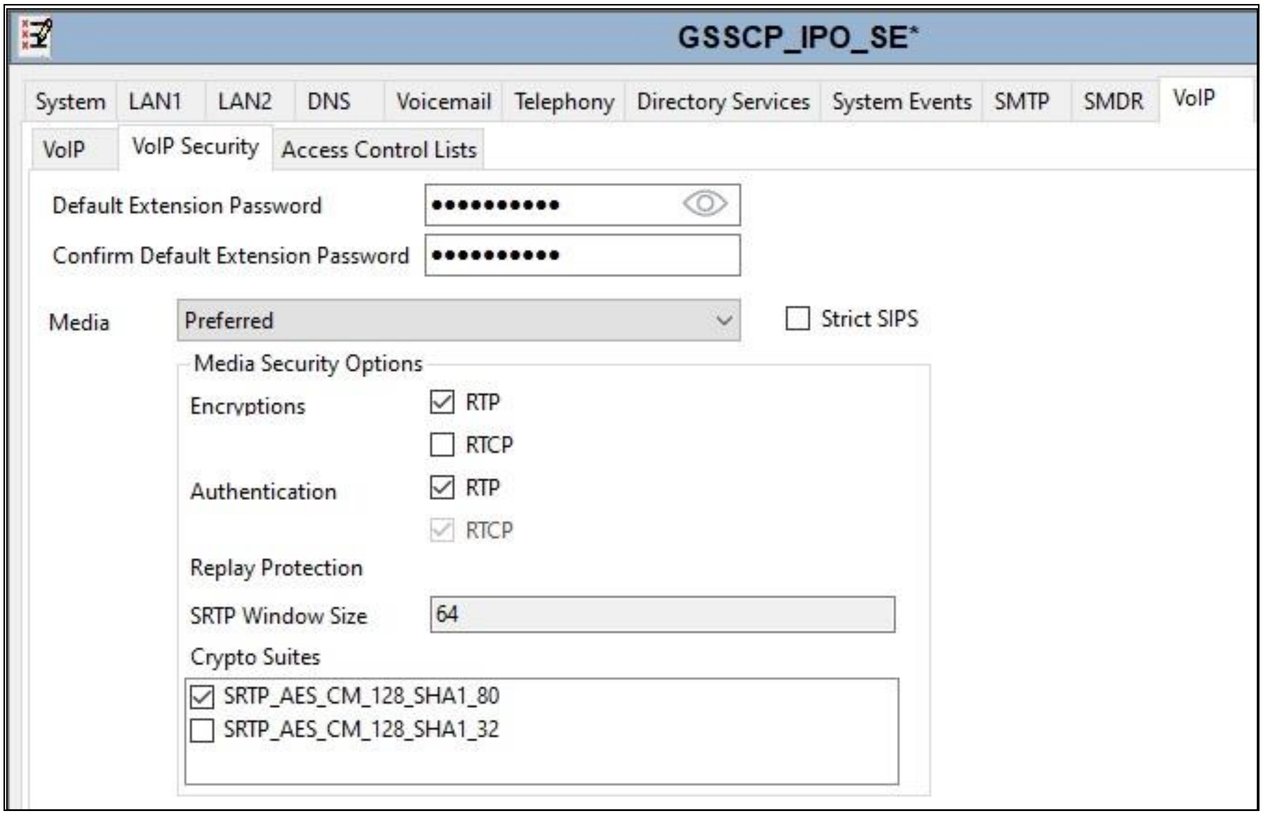
5.5. VoIP Security

When enabling SRTP on the system, the recommended setting for **Media** is **Preferred**. In this scenario, IP Office uses SRTP if supported by the other end, and otherwise uses RTP. If the **Enforced** setting is used, and SRTP is not supported by the other end, the call is not established.

In the compliance testing, **Preferred** is selected as this allows IP Office to fall back to non-secure media if the attempt to use secure media is unsuccessful.

Navigate to **System → VoIP Security** tab and configure as follows:

- Select **Preferred** for **Media**.
- Check **RTP** for **Encryptions**.
- Check **RTP** for **Authentication**.
- Check **SRTP_AES_CM_128_SHA1_80** for **Crypto Suites**.
- Other parameters are left as default.
- Click **OK**.



Default Extension Password ••••••••••
Confirm Default Extension Password ••••••••••
Media Preferred
□ Strict SIPS
Media Security Options
Encryptions ☑ RTP
□ RTCP
Authentication ☑ RTP
☑ RTCP
Replay Protection
SRTP Window Size 64
Crypto Suites
☑ SRTP_AES_CM_128_SHA1_80
□ SRTP_AES_CM_128_SHA1_32

5.6. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Swisscom SIP platform. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.6.1** to create the SIP Line from the template.

Some items relevant to a specific customer environment are not included in the template or may need to be updated after the SIP Line is created. Examples include the following:

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries
- Setting of the **Use Network Topology Info** field on the Transport tab

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary, after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.6.2**.

Also, the following SIP Line settings are not supported on Basic Edition:

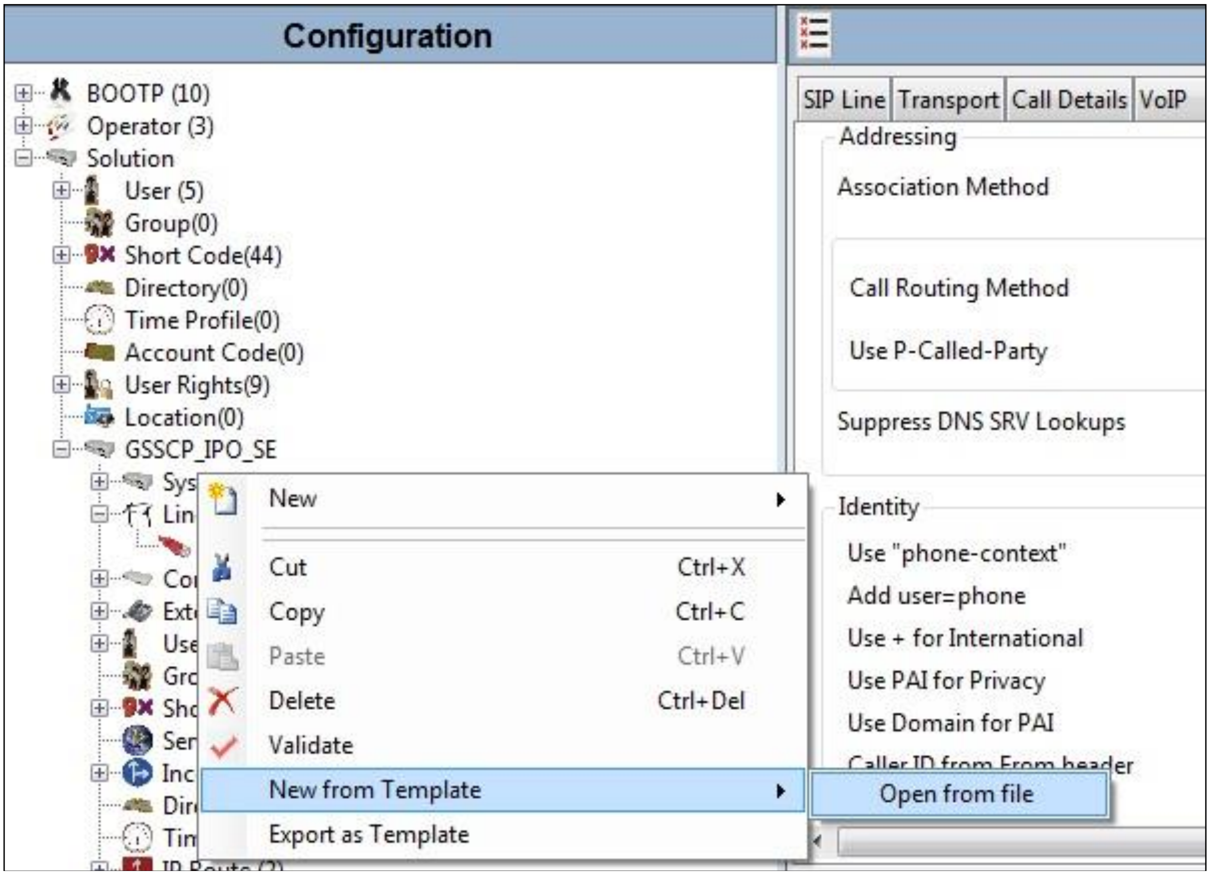
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Section 5.6.2**.

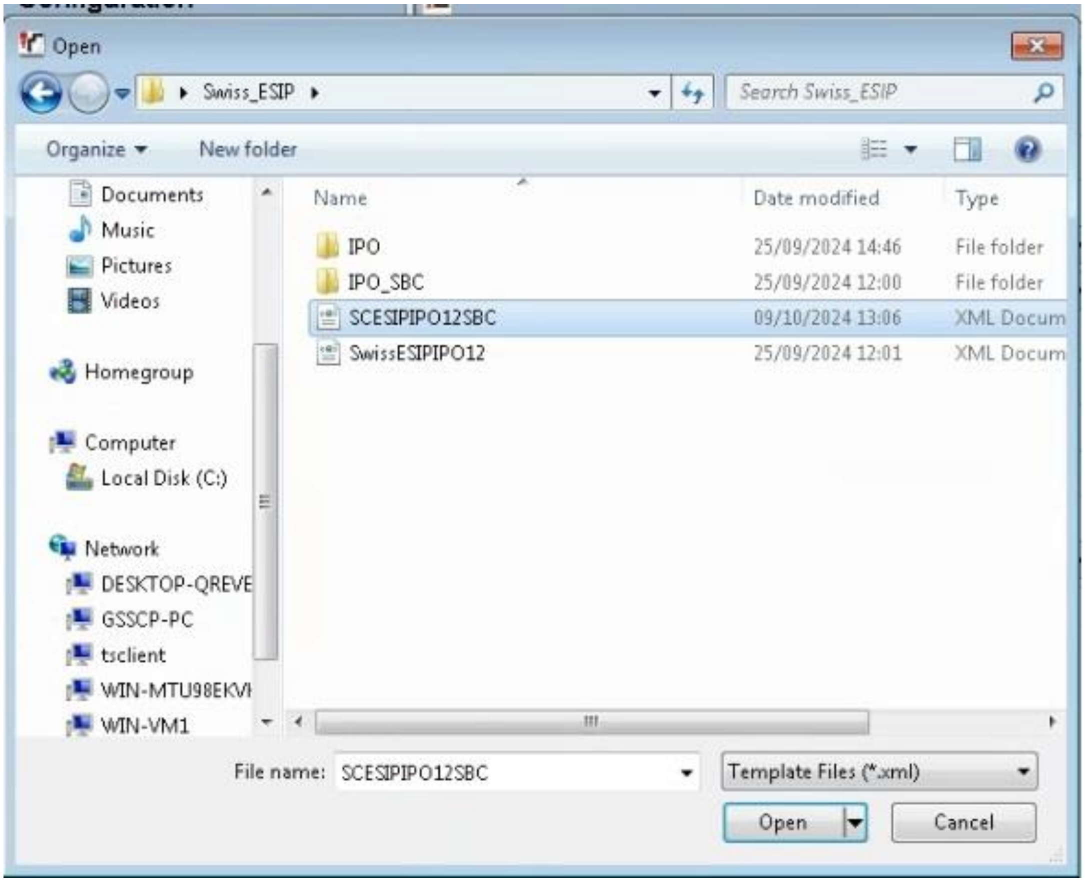
5.6.1. SIP Line From Template

DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

Copy a previously created template file to a location (e.g., *temp*) on the same computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New → New from Template**.



Navigate to the directory on the local machine where the template was copied and select the template as required.



Name	Date modified	Type
IPO	25/09/2024 14:46	File folder
IPO_SBC	25/09/2024 12:00	File folder
SCESIPIPO12SBC	09/10/2024 13:06	XML Docum
SwissESIPIPO12	25/09/2024 12:01	XML Docum

File name: SCESIPIPO12SBC

Template Files (*.xml)

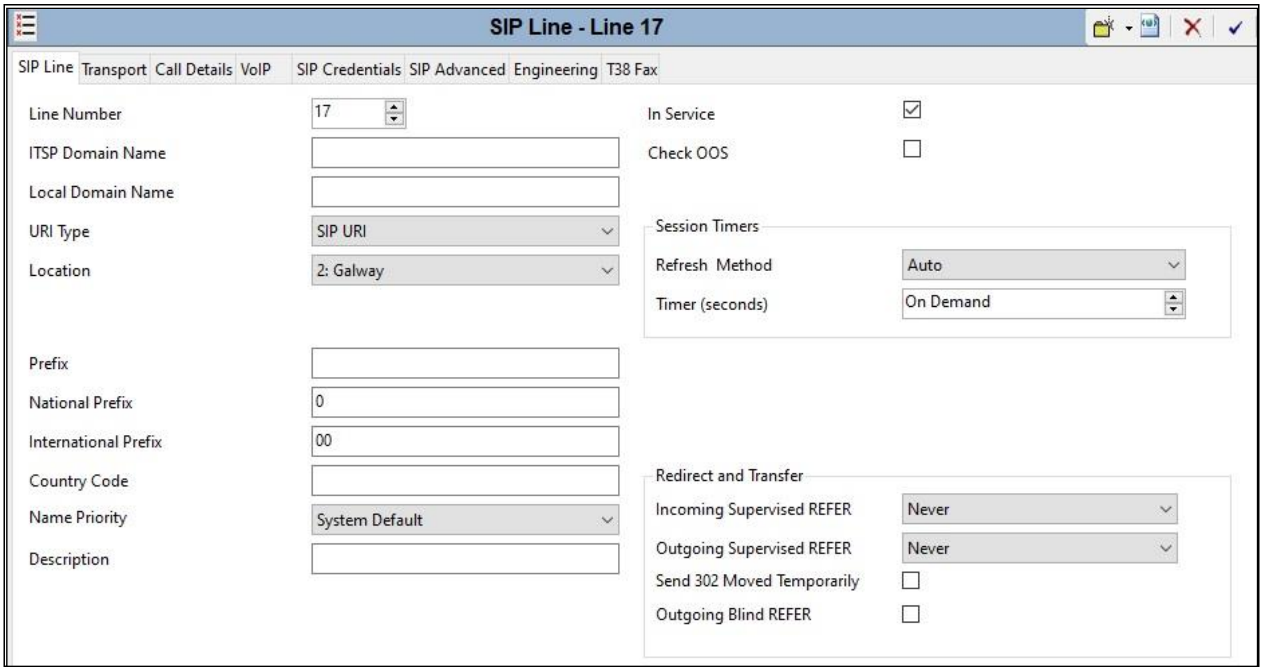
The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.6.2**.

5.6.2. Manual SIP Line Configuration

On the **SIP Line** tab in the Details Pane, configure the parameters below to connect to the SIP Trunking service.

- Set **ITSP Domain Name** to a domain name provider by the Service Provider if required, however no ITSP Domain Name was used in this configuration.
- Set **Location** to that defined for Emergency calls as described in **Section 5.10**.
- Set **National Prefix** to **0** and **International Prefix** to **00** for number conversion as follows: outbound national and international called party numbers are converted to E.164 format; inbound national and international calling party numbers are converted to diallable format.
- Ensure the **In Service** box is checked.
- Leave the **Refresh Method** at the default value of **Auto** which results in re-INVITE being used for Session Refresh.
- Leave **Timer (seconds)** at the default value of **On Demand**. This value allows the Session Refresh interval to be set by the network.
- Set **Incoming Supervised REFER** and **Outgoing Supervise REFER** to **Never**. REFER is not supported by Swisscom SIP platform.
- Default values may be used for all other parameters.

On completion, click the **OK** button (not shown).



Line Number: 17
ITSP Domain Name:
Local Domain Name:
URI Type: SIP URI
Location: 2: Galway
Prefix:
National Prefix: 0
International Prefix: 00
Country Code:
Name Priority: System Default
Description:

In Service ☑
Check OOS □

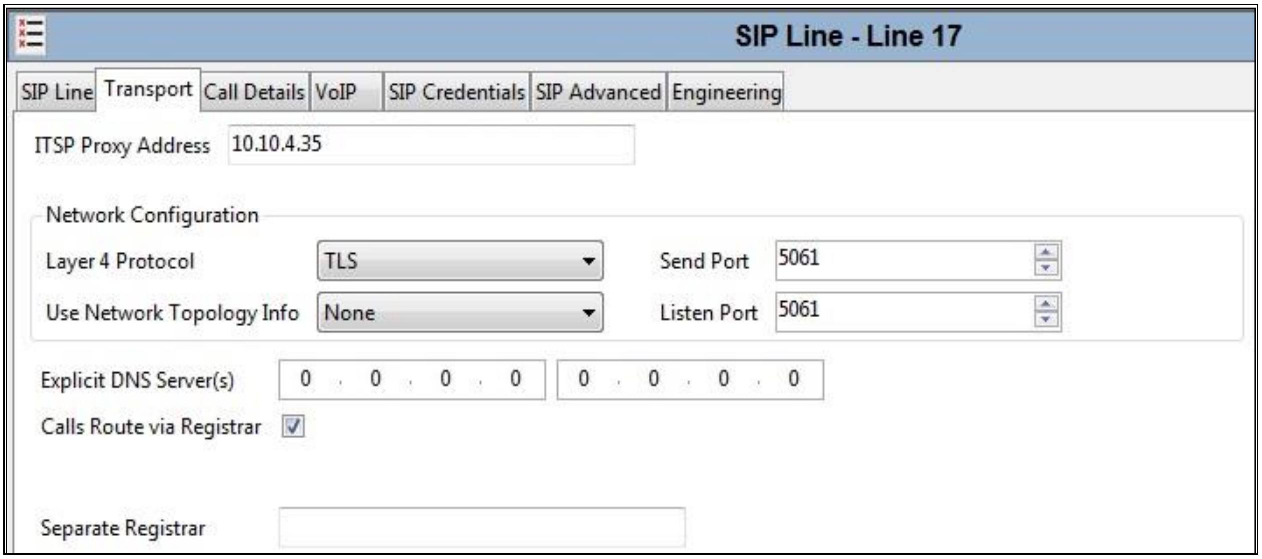
Session Timers
Refresh Method: Auto
Timer (seconds): On Demand

Redirect and Transfer
Incoming Supervised REFER: Never
Outgoing Supervised REFER: Never
Send 302 Moved Temporarily □
Outgoing Blind REFER □

Select the **Transport** tab and set the following:

- Set **ITSP Proxy Address** to the inside interface IP address (**10.10.4.35**) of the Avaya SBC as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **TLS**.
- Set **Send Port** to **5061** and **Listen Port** to **5061**.
- Set **Use Network Topology Info** to **None**.

On completion, click the OK button (not shown).



SIP Line - Line 17

ITSP Proxy Address: 10.10.4.35

Layer 4 Protocol: TLS

Send Port: 5061

Use Network Topology Info: None

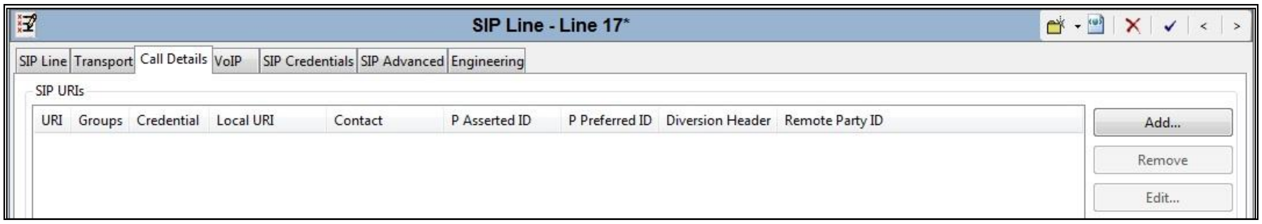
Listen Port: 5061

Explicit DNS Server(s): 0 . 0 . 0 . 0   0 . 0 . 0 . 0

Calls Route via Registrar: ☑

Separate Registrar:

After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, select the **Call Details** tab and click on **Add**.



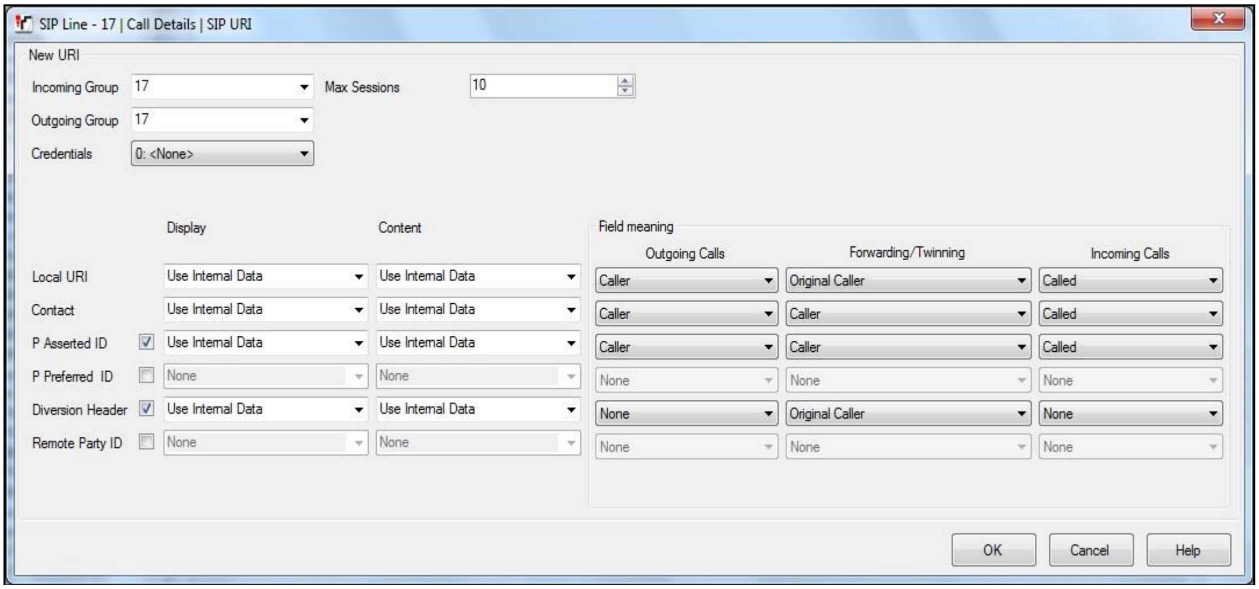
SIP Line - Line 17*

URI	Groups	Credential	Local URI	Contact	P Asserted ID	P Preferred ID	Diversion Header	Remote Party ID

A SIP URI is shown in this example that is used for calls to and from extensions that have a DDI number assigned to them. Additional SIP URI's may be required for calls to services such as Voicemail Collect and the Mobile Twinning FNE, these would be for incoming calls only.

For the compliance test, SIP URI entries were created that matched any number assigned to an Avaya IP Office user. The entry was created with the parameters shown below.

- Set **Incoming Group**. This is the value assigned for incoming calls that are analysed in the Incoming Call Route settings described in **Section 5.9**. In the test environment a value of **17** was used for the Swisscom SIP platform.
- Set **Outgoing Group**. This is the value assigned for outgoing calls that can be selected directly in the short code settings described in **Section 5.7**. In the test environment a value of **17** was used.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern
- Set **Local URI**, **Contact** and **P Asserted ID** to **Use Internal Data** for both the **Display** name and **Content**. On incoming calls, this will analyse the Request-Line sent by Swisscom and match to the SIP settings in the User profile as described in **Section 5.8**. On outgoing calls this will insert the SIP settings in the User profile into the relevant headers in the SIP messages.
- Set the **Outgoing Calls**, **Forwarding/Twinning** and **Incoming Calls** at their respective values of **Caller**, **Original Caller** and **Called** for the **Local URI** setting call details. Set the **Outgoing Calls**, **Forwarding/Twinning** and **Incoming Calls** at their respective values of **Caller**, **Caller** and **Called** for the **Contact** and **P Asserted ID** setting call details. Set the **Outgoing Calls**, **Forwarding/Twinning** and **Incoming Calls** at their respective values of **None**, **Original Caller** and **None** for the **Diversion Header** setting call details.



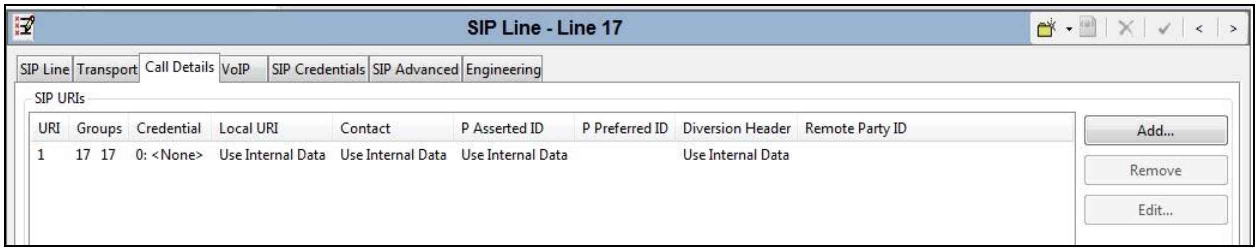
SIP Line - 17 | Call Details | SIP URI

New URI

Incoming Group: 17
Max Sessions: 10
Outgoing Group: 17
Credentials: 0: <None>

		Display	Content	Outgoing Calls	Forwarding/Twinning	Incoming Calls
				Field meaning		
Local URI		Use Internal Data	Use Internal Data	Caller	Original Caller	Called
Contact		Use Internal Data	Use Internal Data	Caller	Caller	Called
P Asserted ID	☑	Use Internal Data	Use Internal Data	Caller	Caller	Called
P Preferred ID	☐	None	None	None	None	None
Diversion Header	☑	Use Internal Data	Use Internal Data	None	Original Caller	None
Remote Party ID	☐	None	None	None	None	None

The following screenshot shows the completed configuration:

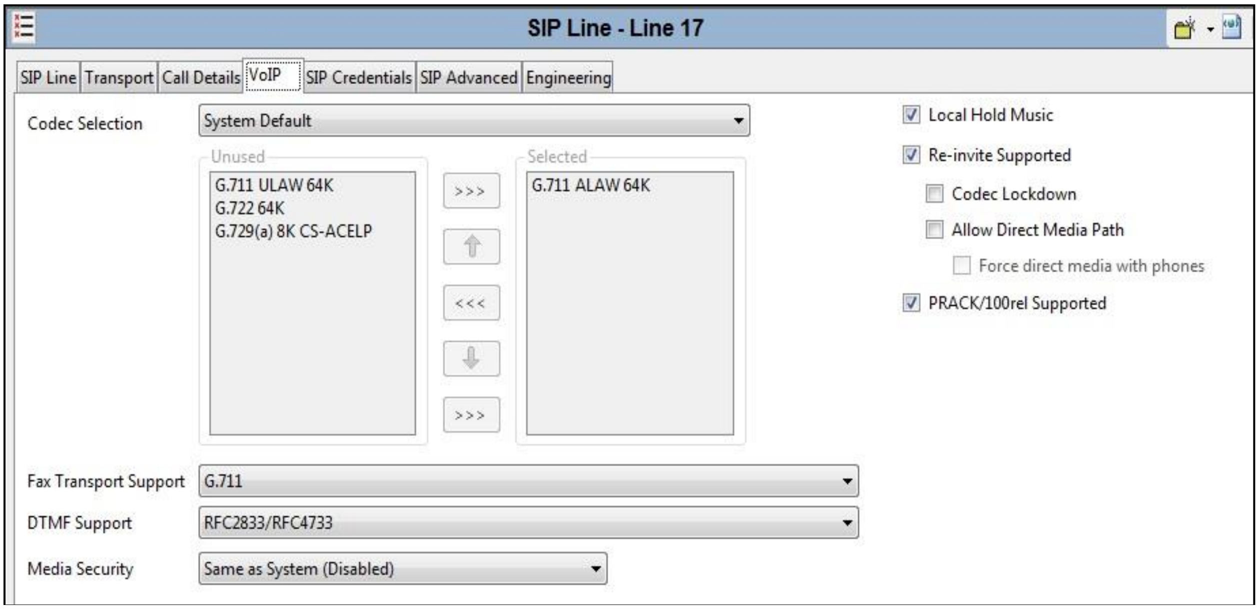


URI	Groups	Credential	Local URI	Contact	P Asserted ID	P Preferred ID	Diversion Header	Remote Party ID
1	17 17	0: <None>	Use Internal Data	Use Internal Data	Use Internal Data		Use Internal Data	

Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- Select **System Default** from the drop-down menu as system default codecs were already defined in **Section 5.4**.
- Set the **Fax Transport Support** box to **G.711** as this is the preferred method of fax transmission for Swisscom.
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Check **Media Security** to **Same as System (Preferred)** and ensure that the **Same as System** box is checked. This ensures that system level media security is set to **Preferred** specifying that SRTP is preferred over RTP as configured in **Section 5.5**.
- Check the **Local Hold Music** box.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of the incoming call or transfer does not support the codec originally negotiated.
- Check the **PRACK/100rel Supported** box if early media is required. This was checked during compliance testing.
- On completion, click the **OK** button (not shown).

Default values may be used for all other parameters.



SIP Line - Line 17

Codec Selection: System Default

Unused: G.711 ULAW 64K, G.722 64K, G.729(a) 8K CS-ACELP

Selected: G.711 ALAW 64K

☑ Local Hold Music

☑ Re-invite Supported

□ Codec Lockdown

□ Allow Direct Media Path

□ Force direct media with phones

☑ PRACK/100rel Supported

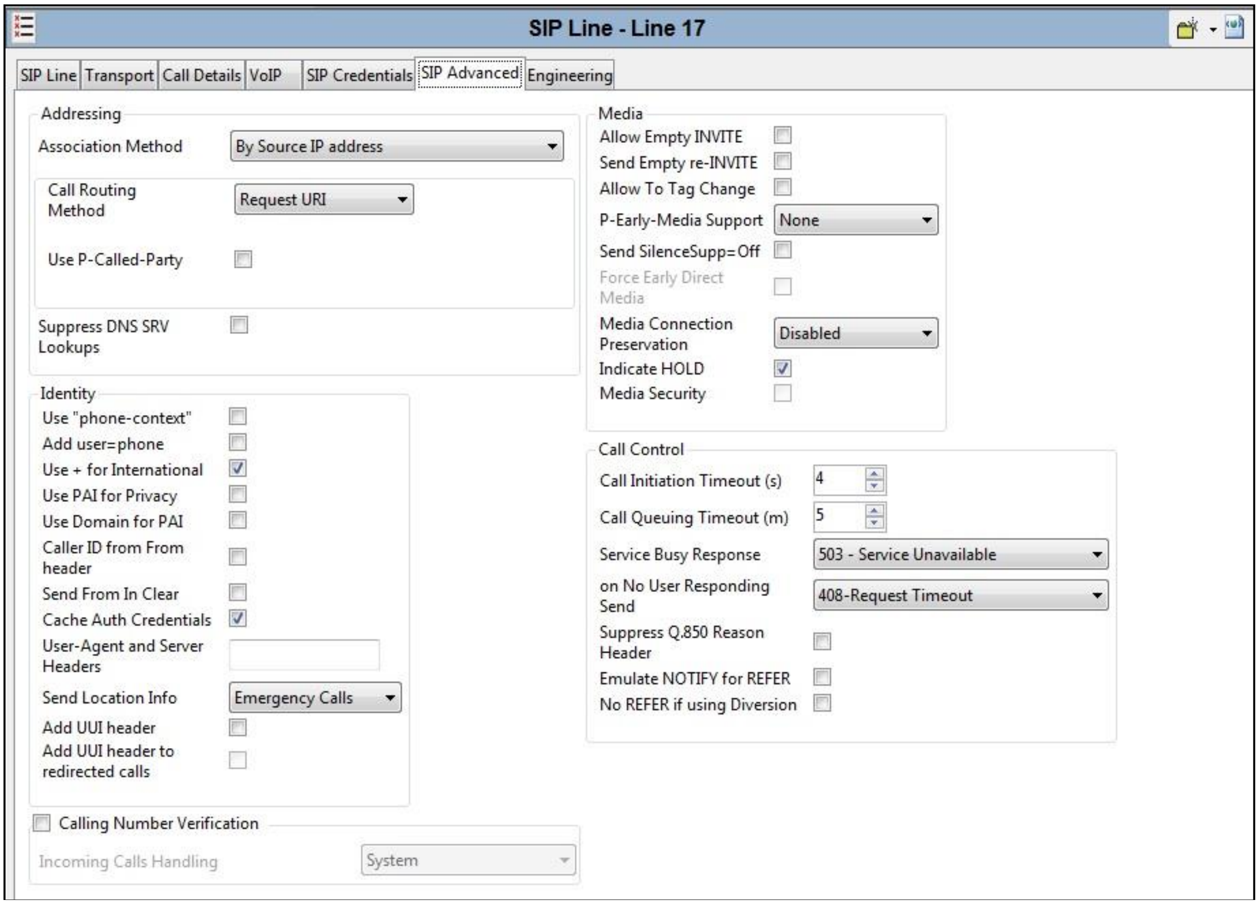
Fax Transport Support: G.711

DTMF Support: RFC2833/RFC4733

Media Security: Same as System (Disabled)

Select the **SIP Advanced** tab and set the following:

- Check the **Use + for International** as E.164 numbering is used on the SIP Trunk.
- Select **Emergency Calls** from the **Send Location Info** drop down menu if required
- Default values may be used for all other parameters.



Addressing
Association Method: By Source IP address
Call Routing Method: Request URI
Use P-Called-Party □
Suppress DNS SRV Lookups □

Identity
Use "phone-context" □
Add user=phone □
Use + for International ☑
Use PAI for Privacy □
Use Domain for PAI □
Caller ID from From header □
Send From In Clear □
Cache Auth Credentials ☑
User-Agent and Server Headers:
Send Location Info: Emergency Calls
Add UUI header □
Add UUI header to redirected calls □

□ Calling Number Verification
Incoming Calls Handling: System

Media
Allow Empty INVITE □
Send Empty re-INVITE □
Allow To Tag Change □
P-Early-Media Support: None
Send SilenceSupp=Off □
Force Early Direct Media □
Media Connection Preservation: Disabled
Indicate HOLD ☑
Media Security □

Call Control
Call Initiation Timeout (s): 4
Call Queuing Timeout (m): 5
Service Busy Response: 503 - Service Unavailable
on No User Responding Send: 408-Request Timeout
Suppress Q.850 Reason Header □
Emulate NOTIFY for REFER □
No REFER if using Diversion □

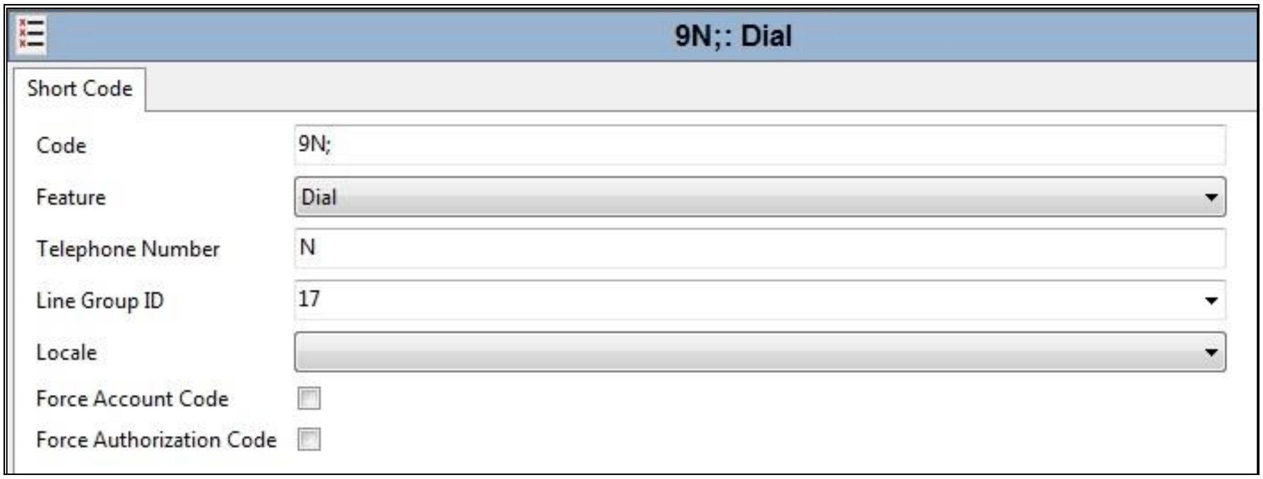
Note: It is advisable at this stage to save the configuration as described in **Section 5.12** to add the Line Group ID defined in **Section 5.6.2** available.

5.7. Short Codes

Define a short code to route outbound traffic to the SIP line and route incoming calls from mobility extensions to access Feature Name Extensions (FNE) hosted on IP Office. To create a short code, right-click **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as shown below.

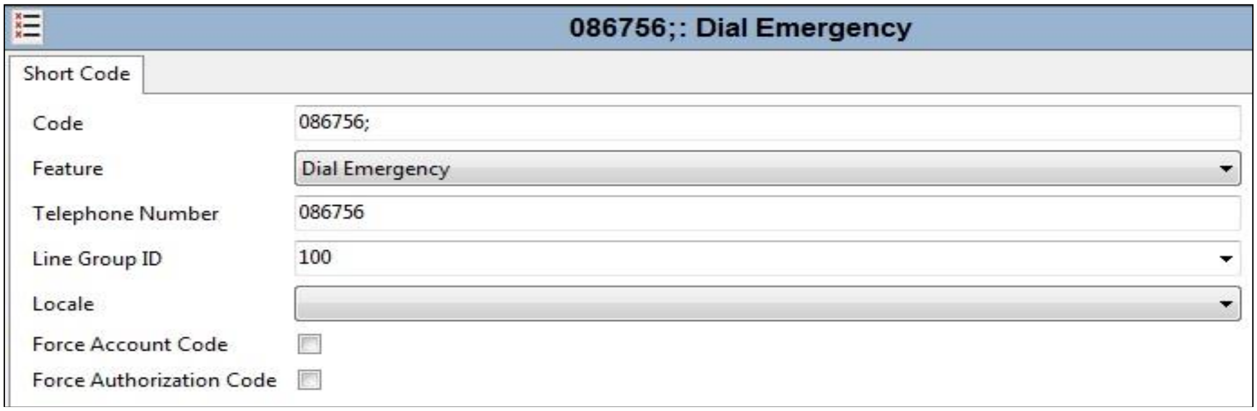
- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. The example shows **9N**; which will be invoked when the user dials 9 followed by the dialled number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **N**. The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message.
- Set the **Line Group Id** to the outgoing line group number defined on the SIP URI tab on the SIP Line in **Section 5.6.2**.

On completion, click the **OK** button (not shown).



Code	9N;
Feature	Dial
Telephone Number	N
Line Group ID	17
Locale	
Force Account Code	□
Force Authorization Code	□

A further example is shown for an emergency number.



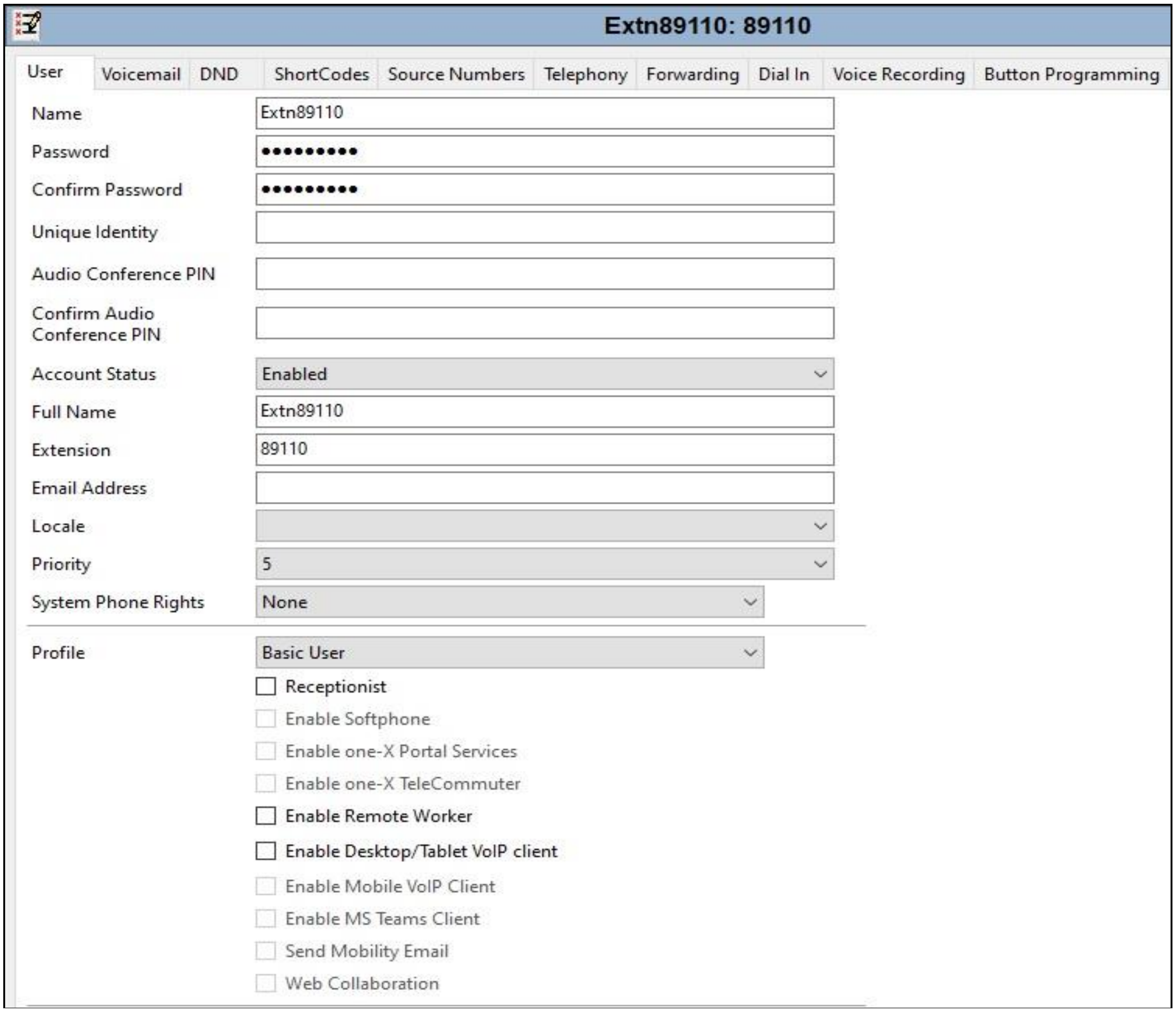
Code	086756;
Feature	Dial Emergency
Telephone Number	086756
Line Group ID	100
Locale	
Force Account Code	□
Force Authorization Code	□

5.8. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.6.2**. To configure these settings, first navigate to **User** in the Navigation Pane. Select the **User** tab if any changes are required.

The following example shows the configuration required for a SIP Endpoint.

- Change the **Name** of the User if required.
- Set the **Password** and **Confirm Password**.
- Select the required profile from the **Profile** drop down menu. **Basic User** is commonly used; **Power User** can be selected for SIP softphone, WebRTC and Remote Worker endpoints.



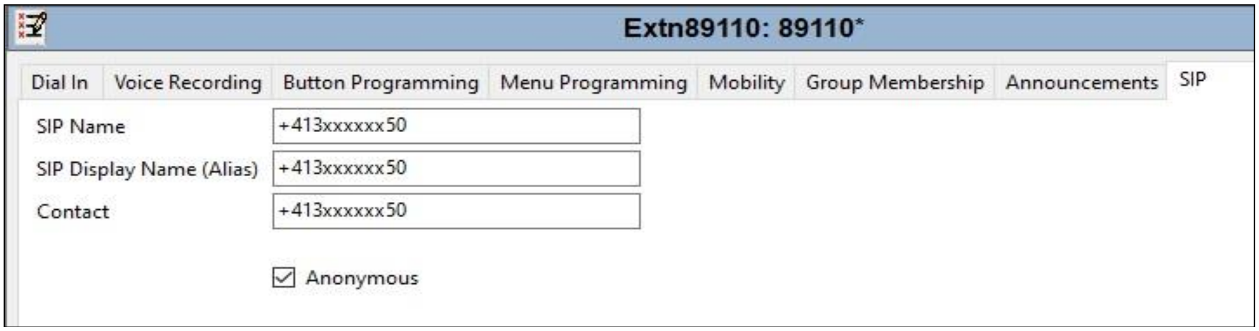
Extn89110: 89110

Name	Extn89110
Password	••••••••••
Confirm Password	••••••••••
Unique Identity	
Audio Conference PIN	
Confirm Audio Conference PIN	
Account Status	Enabled
Full Name	Extn89110
Extension	89110
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Basic User

☐ Receptionist
☐ Enable Softphone
☐ Enable one-X Portal Services
☐ Enable one-X TeleCommuter
☐ Enable Remote Worker
☐ Enable Desktop/Tablet VoIP client
☐ Enable Mobile VoIP Client
☐ Enable MS Teams Client
☐ Send Mobility Email
☐ Web Collaboration

SIP endpoints require setting of the **SIP Registrar Enable** as described in **Section 5.2**.

Next, select the **SIP** tab in the Details Pane. To reach the **SIP** tab click the right arrow on the right-hand side of the Details Pane until it becomes visible. The values entered for the SIP **Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. These allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.6.2)**. As such, these fields should be set to one of the DDI numbers assigned to the enterprise from Swisscom.



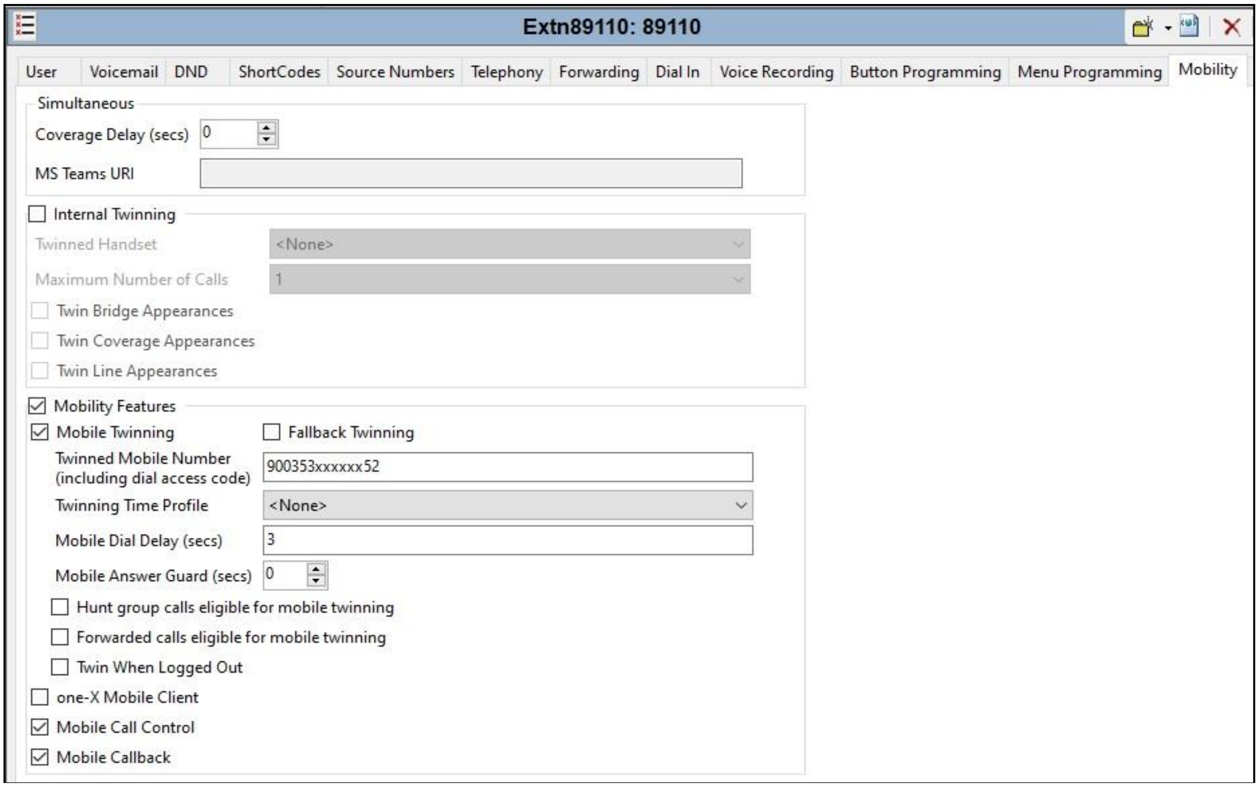
Extn89110: 89110*

SIP Name	+413xxxxxx50
SIP Display Name (Alias)	+413xxxxxx50
Contact	+413xxxxxx50

☑ Anonymous

Note: The **Anonymous** box can be used to restrict Calling Line Identity (CLIR).

The following screen shows the Mobility tab for user 89110. The **Mobility Features** and **Mobile Twinning** are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone over the SIP Trunk. Other options can be set accordingly to customer requirements.



Extn89110: 89110

Simultaneous

Coverage Delay (secs)	0
MS Teams URI	

☐ Internal Twinning

Twinned Handset	<None>
Maximum Number of Calls	1

☐ Twin Bridge Appearances
☐ Twin Coverage Appearances
☐ Twin Line Appearances

☑ Mobility Features
☑ Mobile Twinning ☐ Fallback Twinning

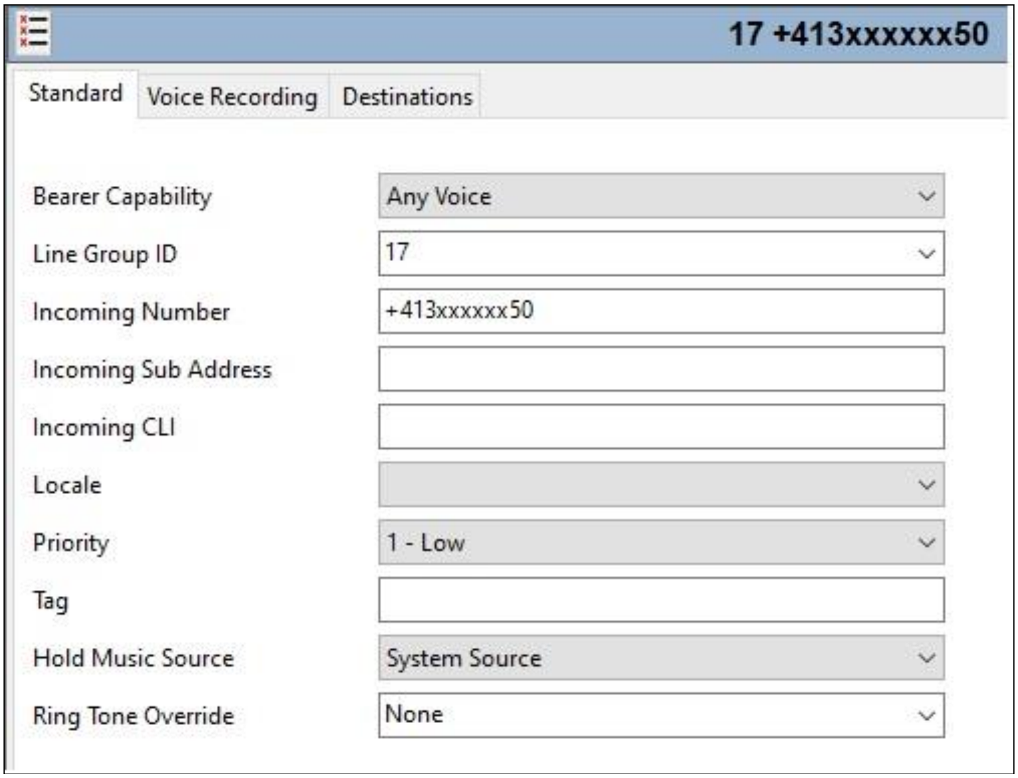
Twinned Mobile Number (including dial access code)	900353xxxxxx52
Twinning Time Profile	<None>
Mobile Dial Delay (secs)	3
Mobile Answer Guard (secs)	0

☐ Hunt group calls eligible for mobile twinning
☐ Forwarded calls eligible for mobile twinning
☐ Twin When Logged Out
☐ one-X Mobile Client
☑ Mobile Call Control
☑ Mobile Callback

5.9. Incoming Call Routing

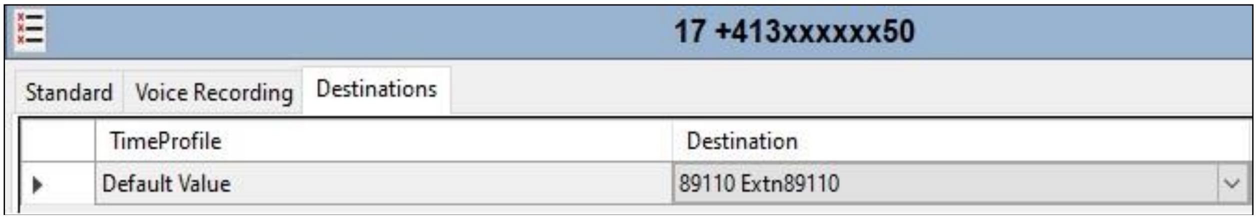
An incoming call route maps an inbound DDI number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.6.2**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left.
- Default values can be used for all other fields.



Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	+413xxxxxx50
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. On completion, click the **OK** button (not shown). In this example, incoming calls to the test DDI number **+413xxxxxx50** on line 17 are routed to extension 89110.

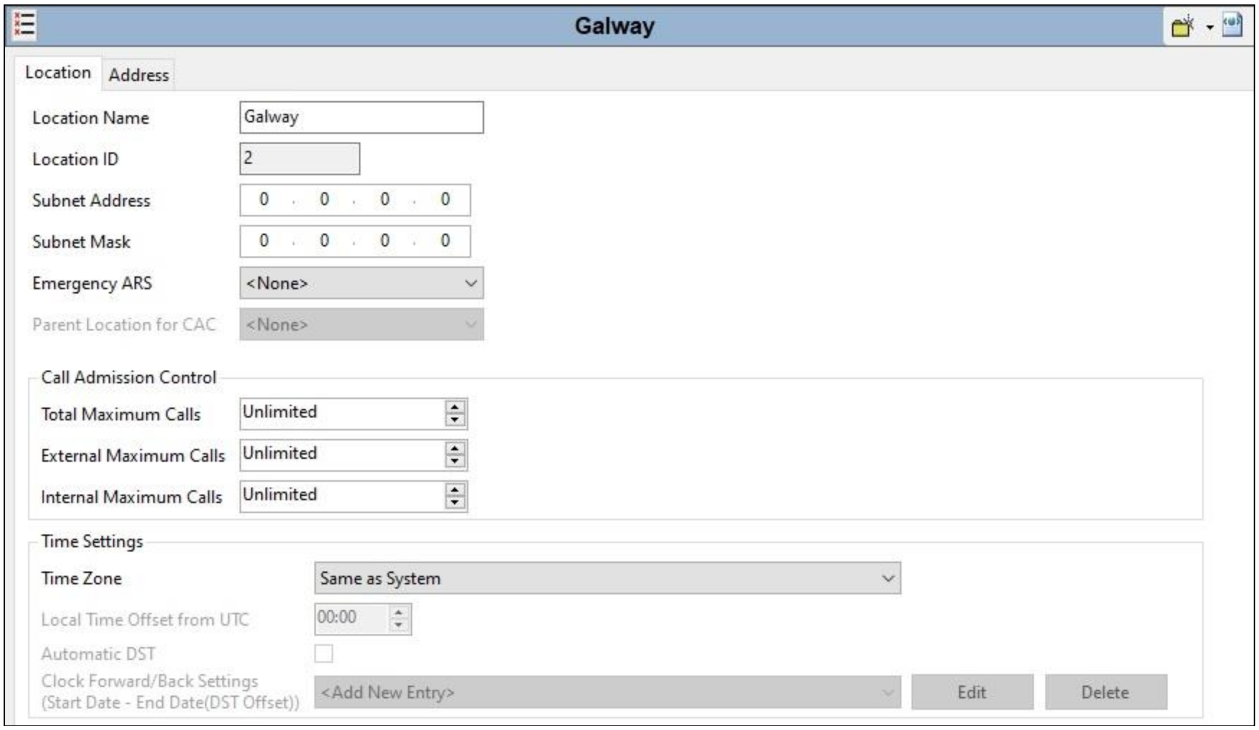


TimeProfile	Destination
Default Value	89110 Extn89110

5.10. Location

If Location information is required for calls to Emergency Services, right-click **Location** in the Navigation Pane and select **New**, (not shown). On the **Location** tab of the Details Pane, enter the parameters as required. An example used during testing is shown below:

- Define a **Location Name**.
- Define a **Subnet Address** and **Subnet Mask** as required. In the test environment, there was no differentiation based on subnet.
- In the example, all other fields were left at default values.



Location Name	Galway
Location ID	2
Subnet Address	0 . 0 . 0 . 0
Subnet Mask	0 . 0 . 0 . 0
Emergency ARS	<None>
Parent Location for CAC	<None>

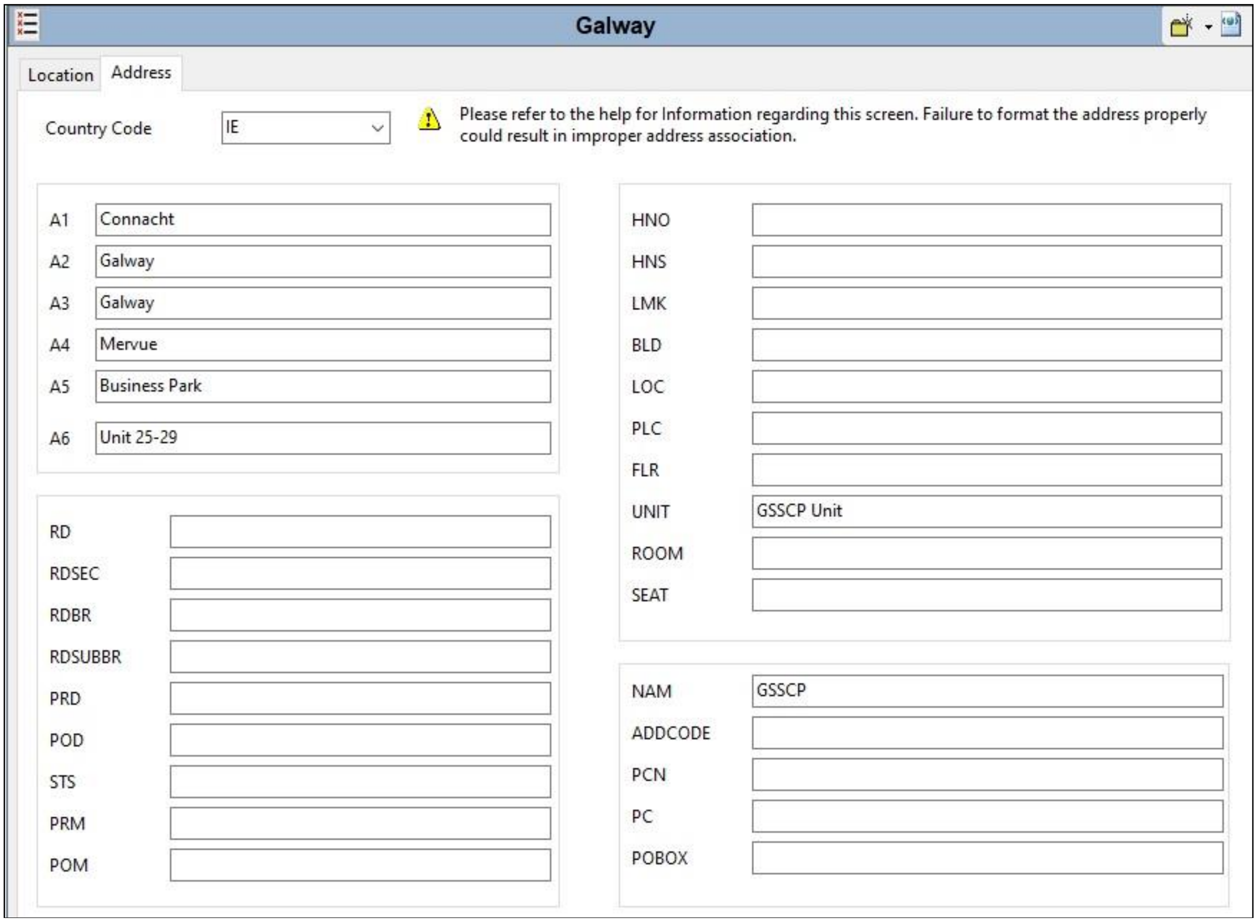
Call Admission Control

Total Maximum Calls	Unlimited
External Maximum Calls	Unlimited
Internal Maximum Calls	Unlimited

Time Settings

Time Zone	Same as System
Local Time Offset from UTC	00:00
Automatic DST	□
Clock Forward/Back Settings (Start Date - End Date(DST Offset))	<Add New Entry>

Click on the **Address** tab and enter data as required. The following screenshot shows an example used during testing:



Galway

Country Code: IE

Please refer to the help for Information regarding this screen. Failure to format the address properly could result in improper address association.

A1	Connacht
A2	Galway
A3	Galway
A4	Mervue
A5	Business Park
A6	Unit 25-29
RD	
RDSEC	
RDBR	
RDSUBBR	
PRD	
POD	
STS	
PRM	
POM	
HNO	
HNS	
LMK	
BLD	
LOC	
PLC	
FLR	
UNIT	GSSCP Unit
ROOM	
SEAT	
NAM	GSSCP
ADDCODE	
PCN	
PC	
POBOX	

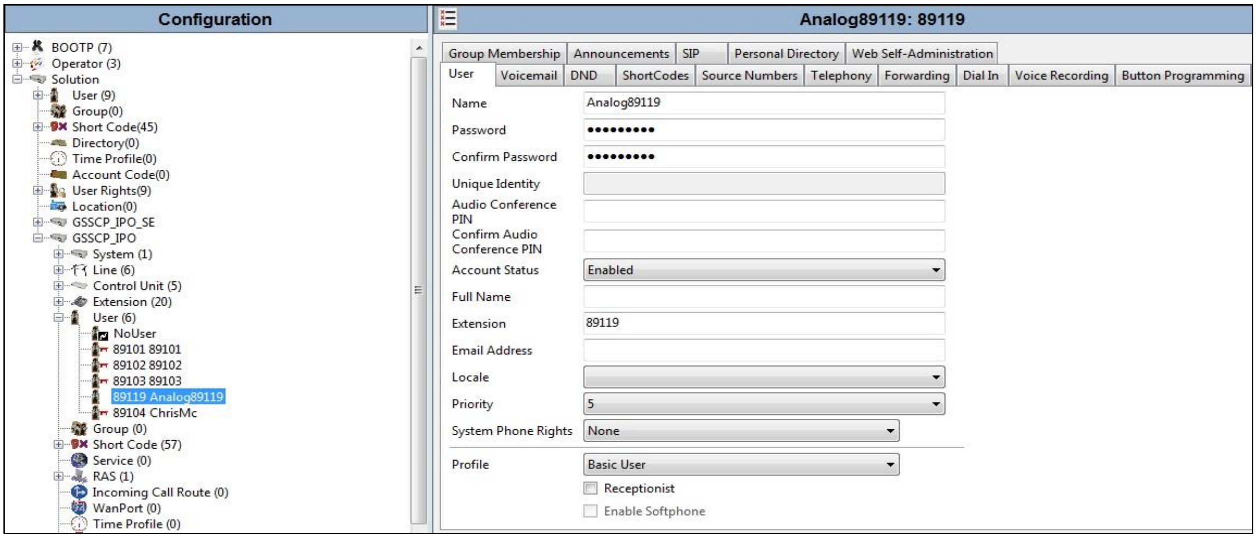
5.11. Fax

At Release 11, both G.711 and T.38 Fax is supported on IP Office Server Edition when using an IP Office Expansion (500 V2). The Swisscom SIP Trunk testing was carried out using this configuration with only the analog extension for the fax machine on the Expansion. In this configuration, the T.38 fax settings are configured on the SIP line between the Expansion and the Server.

5.11.1. Analog User

To configure the settings for the fax User, first navigate to **User** in the Navigation Pane for the Expansion. In the test environment, the 500V2 Expansion is called **GSSCP_IPO**. Select the **User** tab. The following example shows the configuration required for an analog Endpoint.

- Change the **Name** of the User if required.
- The **Password** and **Confirm Password** fields are set but are not required for analog endpoints.
- Select the required profile from the **Profile** drop down menu. **Basic User** is sufficient for fax.



Analog89119: 89119

Name	Analog89119
Password	•••••••••
Confirm Password	•••••••••
Unique Identity	
Audio Conference PIN	
Confirm Audio Conference PIN	
Account Status	Enabled
Full Name	
Extension	89119
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Basic User
	□ Receptionist
	□ Enable Softphone

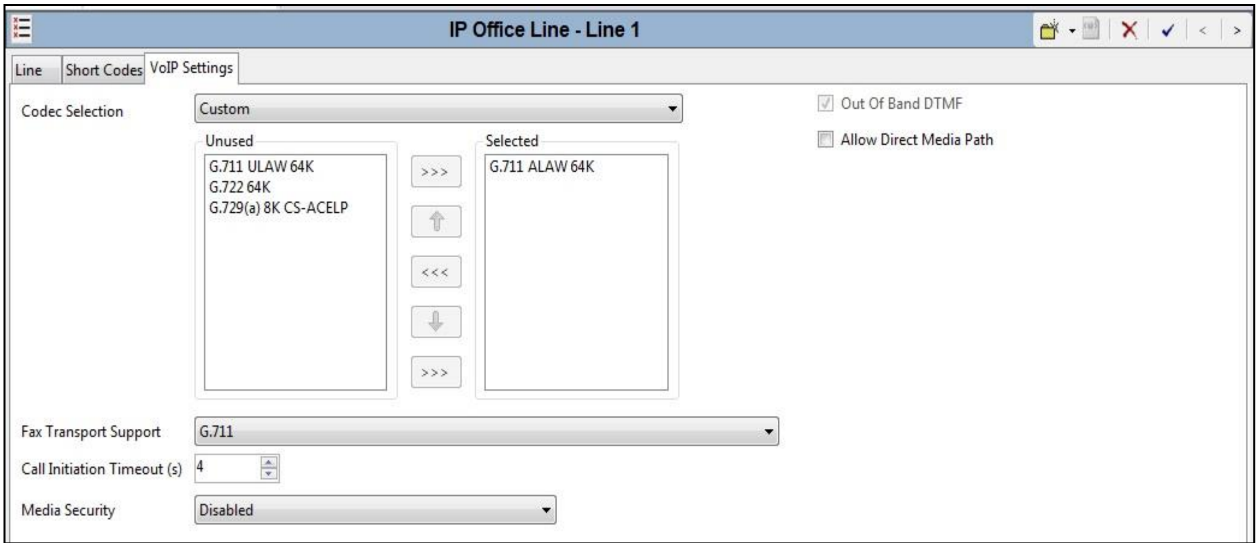
Configure other settings as described in **Section 5.7**.

5.11.2. G.711 Fax Settings

The G.711 Fax settings are defined on the SIP Line between the Expansion and the Server. Note that the VoIP settings for G.711 are required in three places in this configuration:

- The SIP Line for the Swisscom Smart Business Connect SIP platform as described in **Section 5.6.2**.
- The IP Office Line between the Server and the Expansion on the Expansion.
- The IP Office Line between the Server and the Expansion on the Server.

In all the above cases, the **Fax Transport Support** was set to **G711**. The following screenshot shows the VoIP Settings for the IP Office Line between the Server and the Expansion on the Expansion:



IP Office Line - Line 1

Codec Selection: Custom

Unused:
G.711 ULAW 64K
G.722 64K
G.729(a) 8K CS-ACELP

Selected:
G.711 ALAW 64K

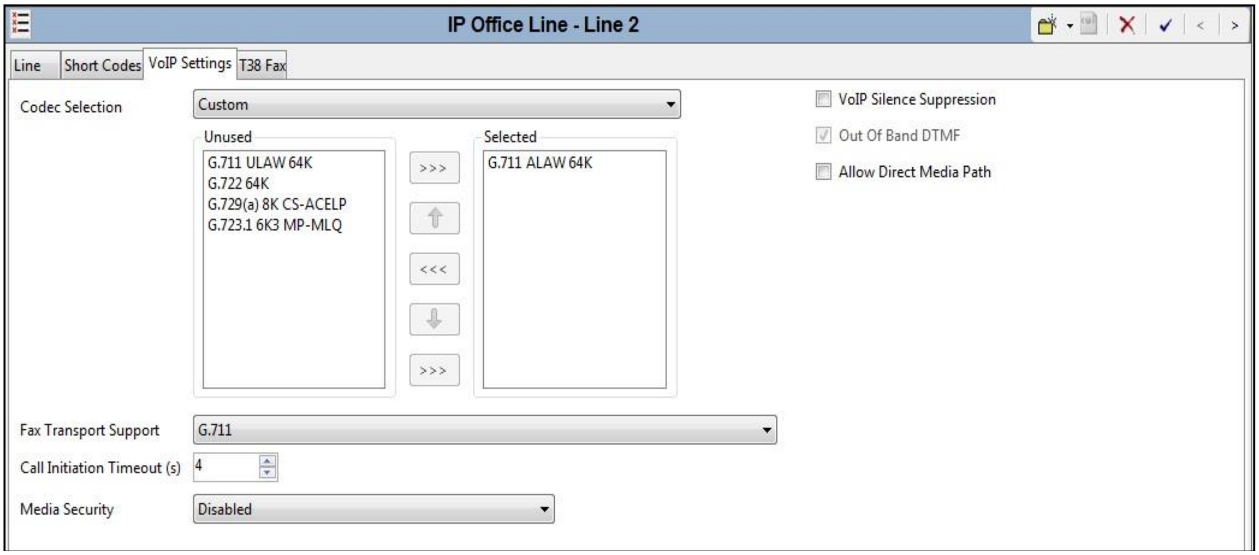
☑ Out Of Band DTMF
□ Allow Direct Media Path

Fax Transport Support: G.711

Call Initiation Timeout (s): 4

Media Security: Disabled

The following shows the **VoIP Settings** tab in the IP Office Line for the Expansion in the Server configuration:



IP Office Line - Line 2

Codec Selection: Custom

Unused:
G.711 ULAW 64K
G.722 64K
G.729(a) 8K CS-ACELP
G.723.1 6K3 MP-MLQ

Selected:
G.711 ALAW 64K

□ VoIP Silence Suppression
☑ Out Of Band DTMF
□ Allow Direct Media Path

Fax Transport Support: G.711

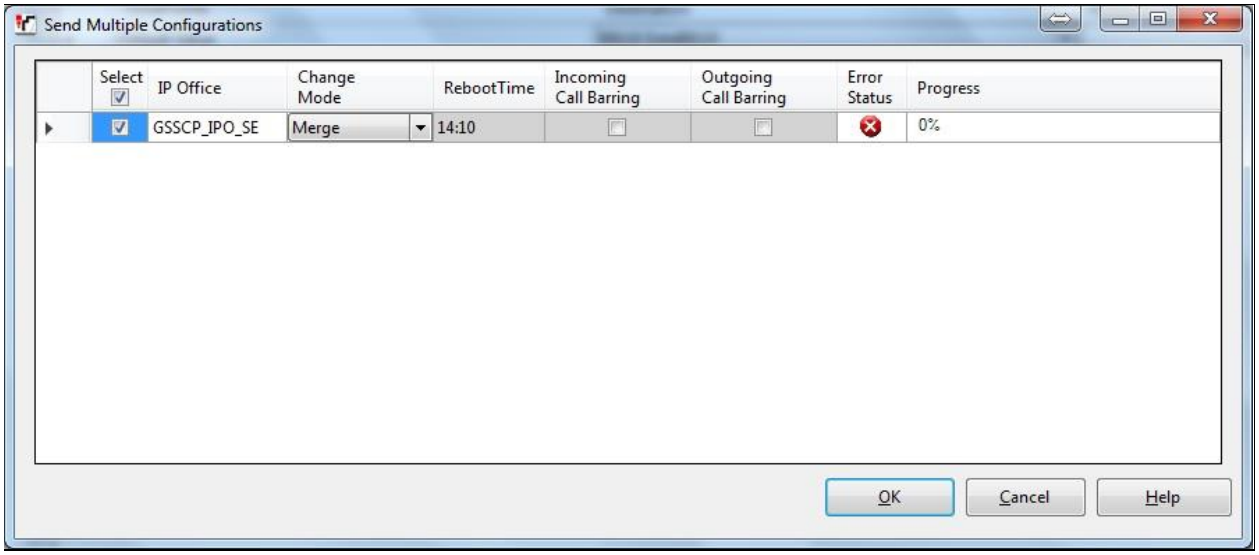
Call Initiation Timeout (s): 4

Media Security: Disabled

Refer to **Section 5.6.2** for the VoIP Settings on the SIP Line for the Swisscom SIP Trunk.

5.12. Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections. A screen like the one shown below is displayed where the system configuration has been changed and needs to be saved on the system. **Merge, Immediate, When Free** or **Timed** is shown under the **Configuration Reboot Mode** column, based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to save the configuration
Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections. A screen like the one shown below is displayed where the system configuration has been changed and needs to be saved on the system. **Merge, Reboot, Timed** or **RebootWhen Free** can be selected from the **Change Mode** drop-down menu based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to save the configuration.



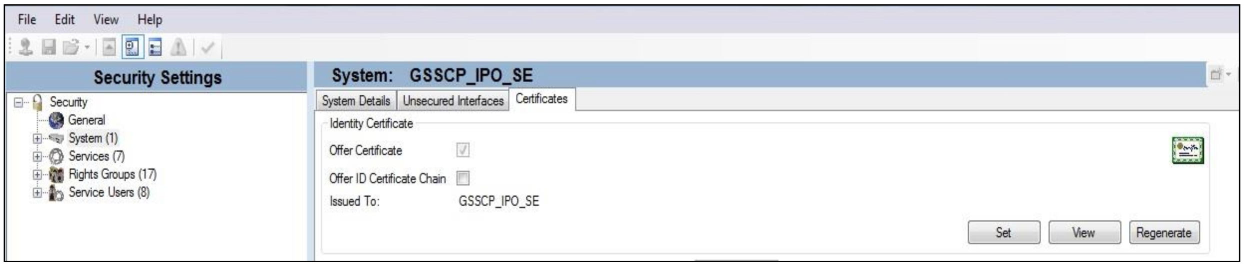
	Select ☑	IP Office	Change Mode	RebootTime	Incoming Call Barring	Outgoing Call Barring	Error Status	Progress
▸	☑	GSSCP_IPO_SE	Merge	14:10	□	□	✖	0%

5.13. TLS Certificates

For the compliance test, TLS signalling was used internally to the enterprise wherever possible. Testing was done using identity certificates signed by a local certificate authority **System Manager CA**. The generation and installation of these certificates are beyond the scope of these Application Notes.

To view the certificate currently installed on IP Office, navigate to **File → Advanced → Security Settings**. In the Security Settings window, navigate to **Security → System** and select the **Certificates** tab.

To verify the identity certificate, locate the **Identity Certificate** section and click **View** to see the details of the certificate.



System: GSSCP_IPO_SE

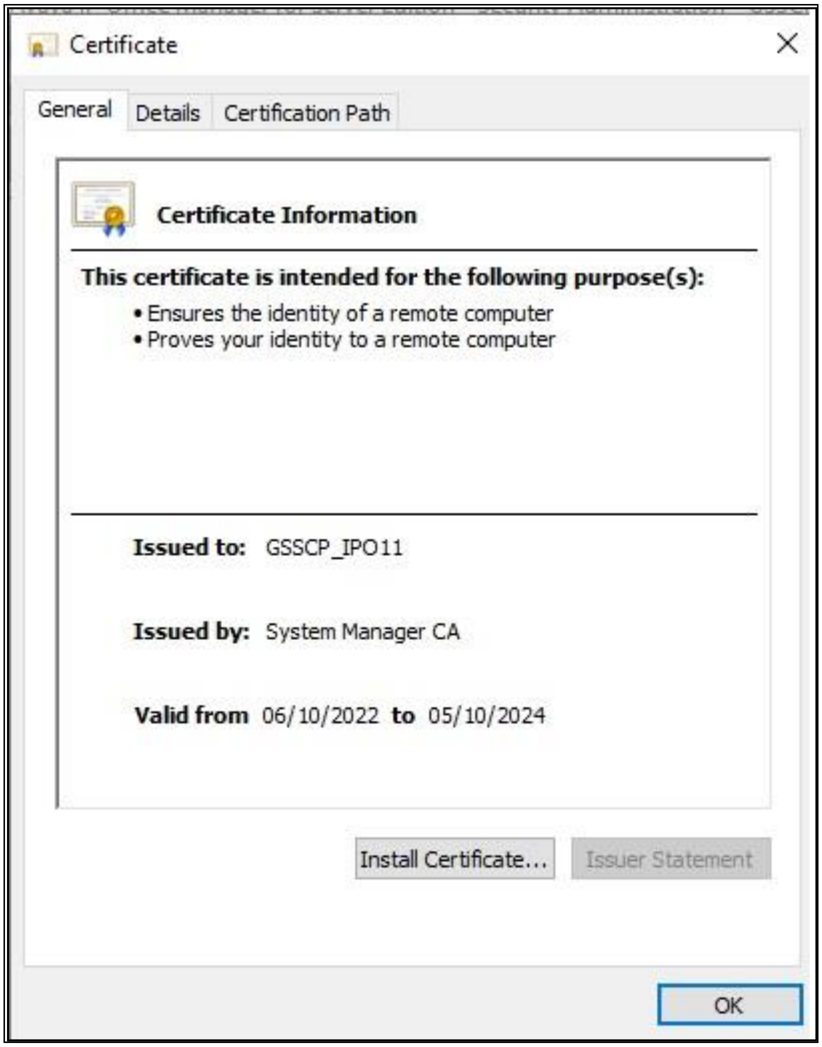
Identity Certificate

Offer Certificate ☑

Offer ID Certificate Chain □

Issued To: GSSCP_IPO_SE

A pop-up window displays the certificate that is issued to the Avaya IP Office (**GSSCP_IPO_SE**) and issued by **System Manager CA**. Click **OK** to close the pop-up window.



Certificate Information

This certificate is intended for the following purpose(s):

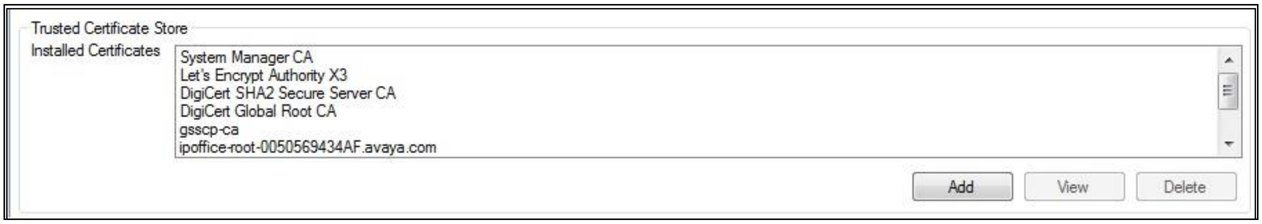
- Ensures the identity of a remote computer
- Proves your identity to a remote computer

Issued to: GSSCP_IPO11

Issued by: System Manager CA

Valid from 06/10/2022 **to** 05/10/2024

To verify the trusted certificates, return to the **Security → System →Certificates** tab and scroll down to the **Trusted Certificate Store** section. Verify that **System Manager CA** is displayed as an **Installed Certificates**.


Trusted Certificate Store

Installed Certificates

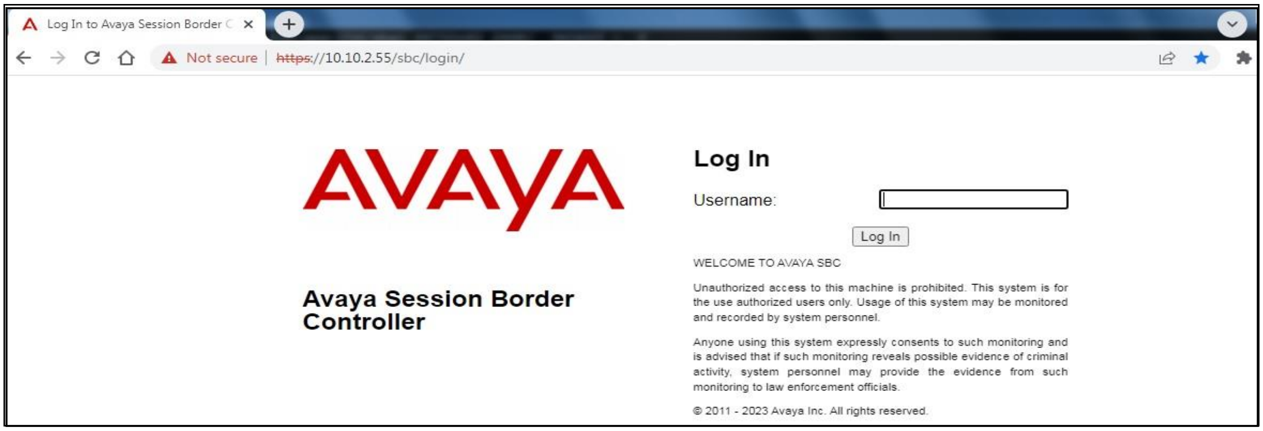
System Manager CA
Let's Encrypt Authority X3
DigiCert SHA2 Secure Server CA
DigiCert Global Root CA
gsscp-ca
ipoffice-root-0050569434AF.avaya.com

6. Configure Avaya Session Border Controller

This section describes the configuration of the Session Border Controller (Avaya SBC). The Avaya SBC provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

6.1. Accessing Avaya Session Border Controller

Access the Avaya SBC using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.


Log In to Avaya Session Border C
Not secure
https://10.10.2.55/sbc/login/
AVAYA
Log In

Avaya Session Border Controller

Log In

Username:

Log In

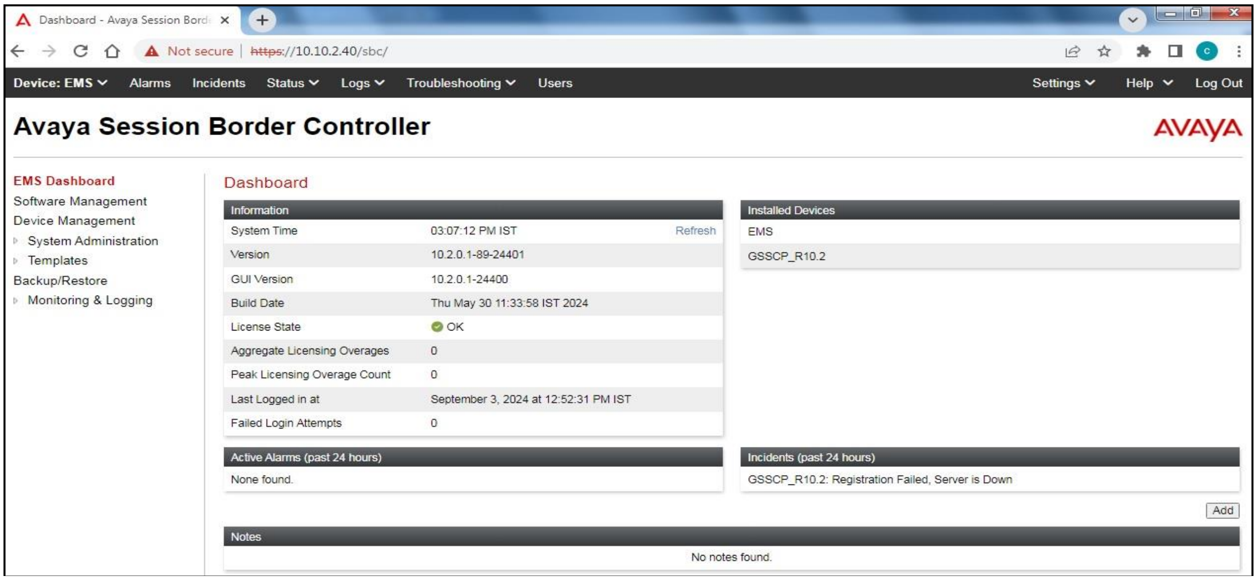
WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2023 Avaya Inc. All rights reserved.

Once logged in, on the top-left of the screen, under **Device:** select the required device from the drop-down menu. with a menu on the left-hand side. In this case, **GSSCP_10.2** is used as a starting point for all configuration of the Avaya SBC.



Avaya Session Border Controller

Dashboard

Information	
System Time	03:07:12 PM IST
Version	10.2.0.1-89-24401
GUI Version	10.2.0.1-24400
Build Date	Thu May 30 11:33:58 IST 2024
License State	✓ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	September 3, 2024 at 12:52:31 PM IST
Failed Login Attempts	0

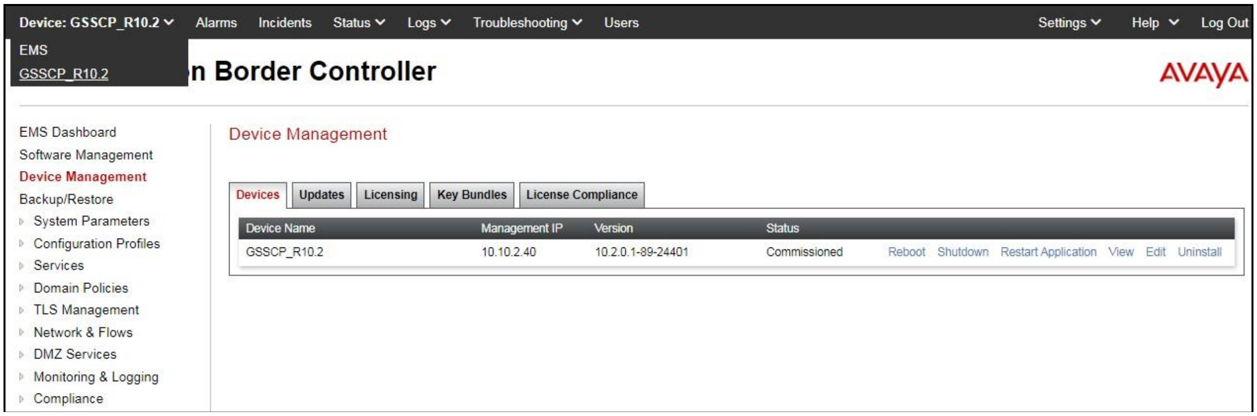
Installed Devices
EMS
GSSCP_R10.2

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
GSSCP_R10.2: Registration Failed, Server is Down

Notes
No notes found.

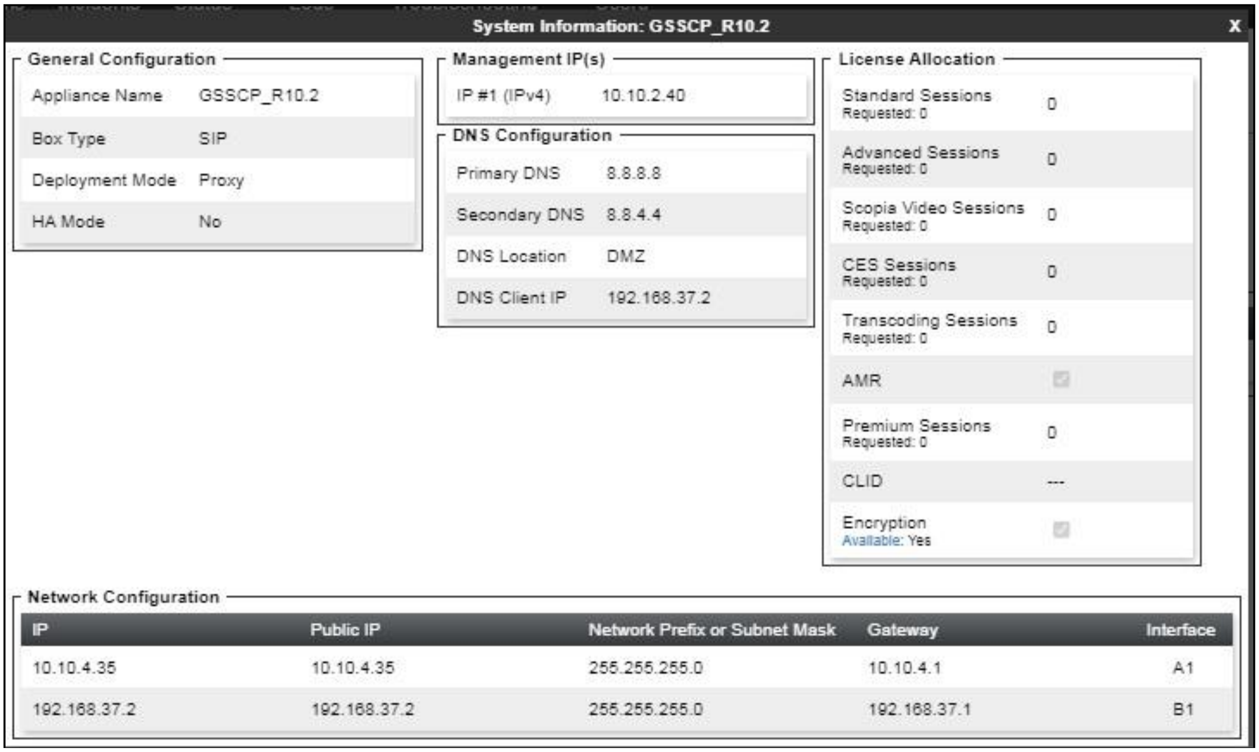
To view system information that was configured during installation, navigate to **Device Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_10.2** is shown. To view the configuration of this device, click **View** (the third option from the right).



Device Management

Device Name	Management IP	Version	Status	
GSSCP_R10.2	10.10.2.40	10.2.0.1-89-24401	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

The **System Information** screen shows the **General Configuration**, **Device Configuration**, **License Allocation**, **Network Configuration**, **DNS Configuration** and **Management IP** information.



System Information: GSSCP_R10.2

General Configuration

Appliance Name	GSSCP_R10.2
Box Type	SIP
Deployment Mode	Proxy
HA Mode	No

Management IP(s)

IP #1 (IPv4)	10.10.2.40

DNS Configuration

Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4
DNS Location	DMZ
DNS Client IP	192.168.37.2

License Allocation

Standard Sessions Requested: 0	0
Advanced Sessions Requested: 0	0
Scopia Video Sessions Requested: 0	0
CES Sessions Requested: 0	0
Transcoding Sessions Requested: 0	0
AMR	☑
Premium Sessions Requested: 0	0
CLID	---
Encryption Available: Yes	☑

Network Configuration

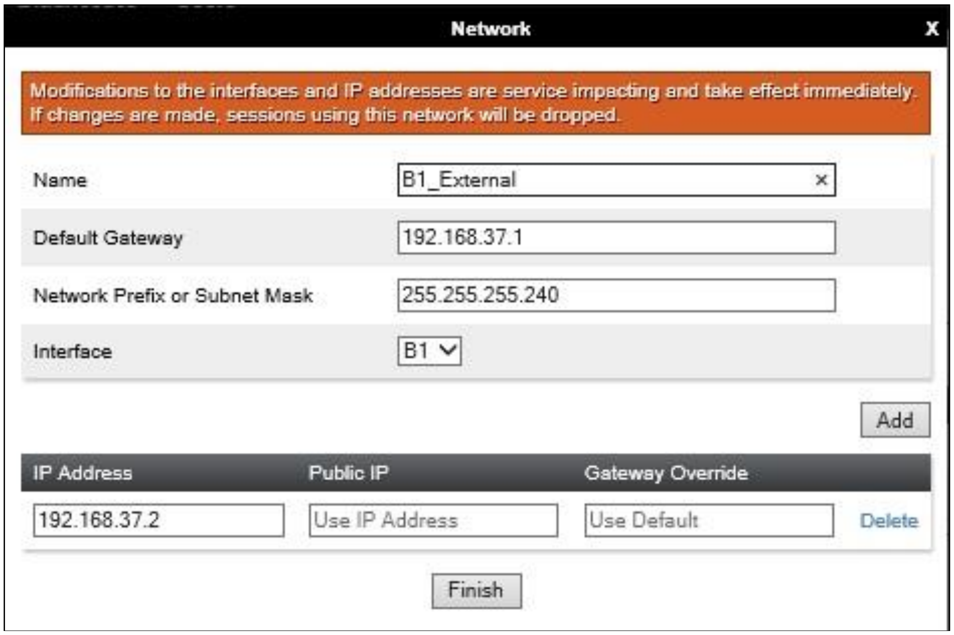
IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.10.4.35	10.10.4.35	255.255.255.0	10.10.4.1	A1
192.168.37.2	192.168.37.2	255.255.255.0	192.168.37.1	B1

6.2. Define Network Management

Network information is required on the Avaya SBC to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBC can have only one physical interface assigned.

To define the network information, navigate to **Network & Flows → Network Management** in the main menu on the left-hand side and click on **Add**. Enter details for the external interfaces in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Network Prefix or Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the test environment, this was **B1.**
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address of the Avaya SBC on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.



Network

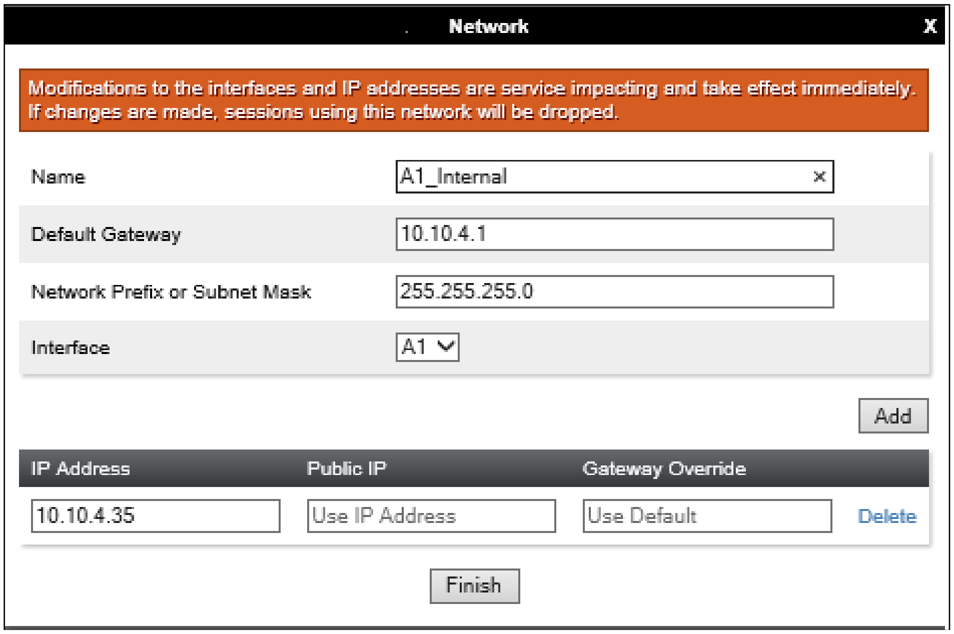
Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped.

Name	B1_External
Default Gateway	192.168.37.1
Network Prefix or Subnet Mask	255.255.255.240
Interface	B1

IP Address	Public IP	Gateway Override	
192.168.37.2	Use IP Address	Use Default	Delete

Click on **Add** to define the internal interfaces or Edit if it was defined during installation of the Avaya SBC. Enter details in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Network Prefix or Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1.**
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address of the Avaya SBC on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.



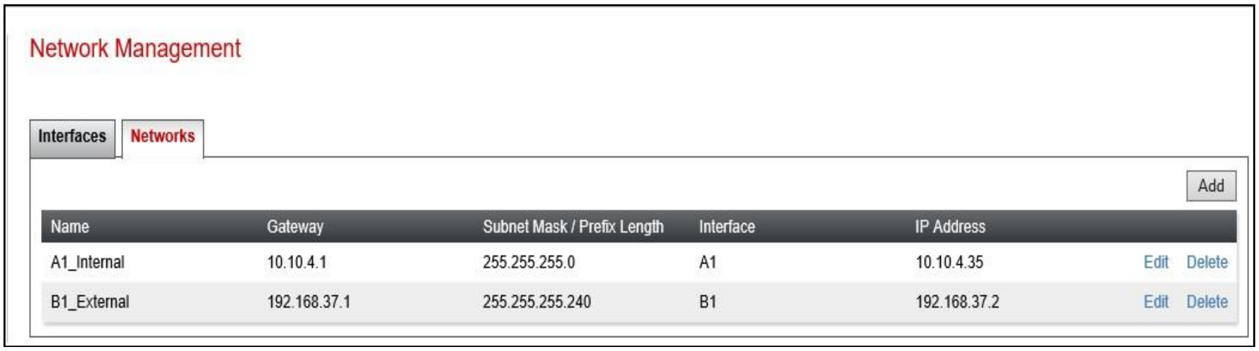
Network

Modifications to the interfaces and IP addresses are service impacting and take effect immediately. If changes are made, sessions using this network will be dropped.

Name	A1_Internal
Default Gateway	10.10.4.1
Network Prefix or Subnet Mask	255.255.255.0
Interface	A1

IP Address	Public IP	Gateway Override	
10.10.4.35	Use IP Address	Use Default	Delete

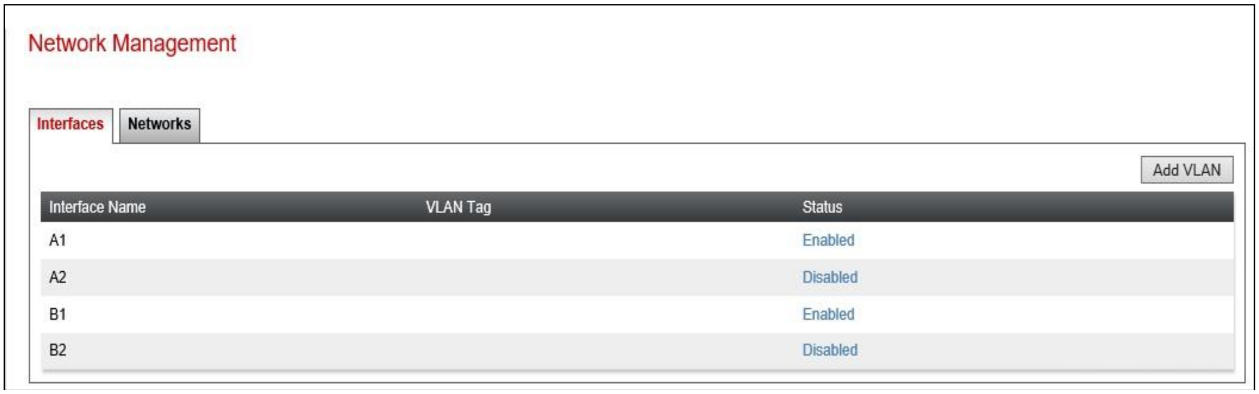
The following screenshot shows the completed Network Management configuration:



Network Management

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
A1_Internal	10.10.4.1	255.255.255.0	A1	10.10.4.35	Edit Delete
B1_External	192.168.37.1	255.255.255.240	B1	192.168.37.2	Edit Delete

Select the **Interfaces** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.



Network Management

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

Note: to ensure that the Avaya SBC uses the interfaces defined, the Application must be restarted.

- Click on **Device Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear that will indicate when the restart is complete.

6.3. Define TLS Profiles

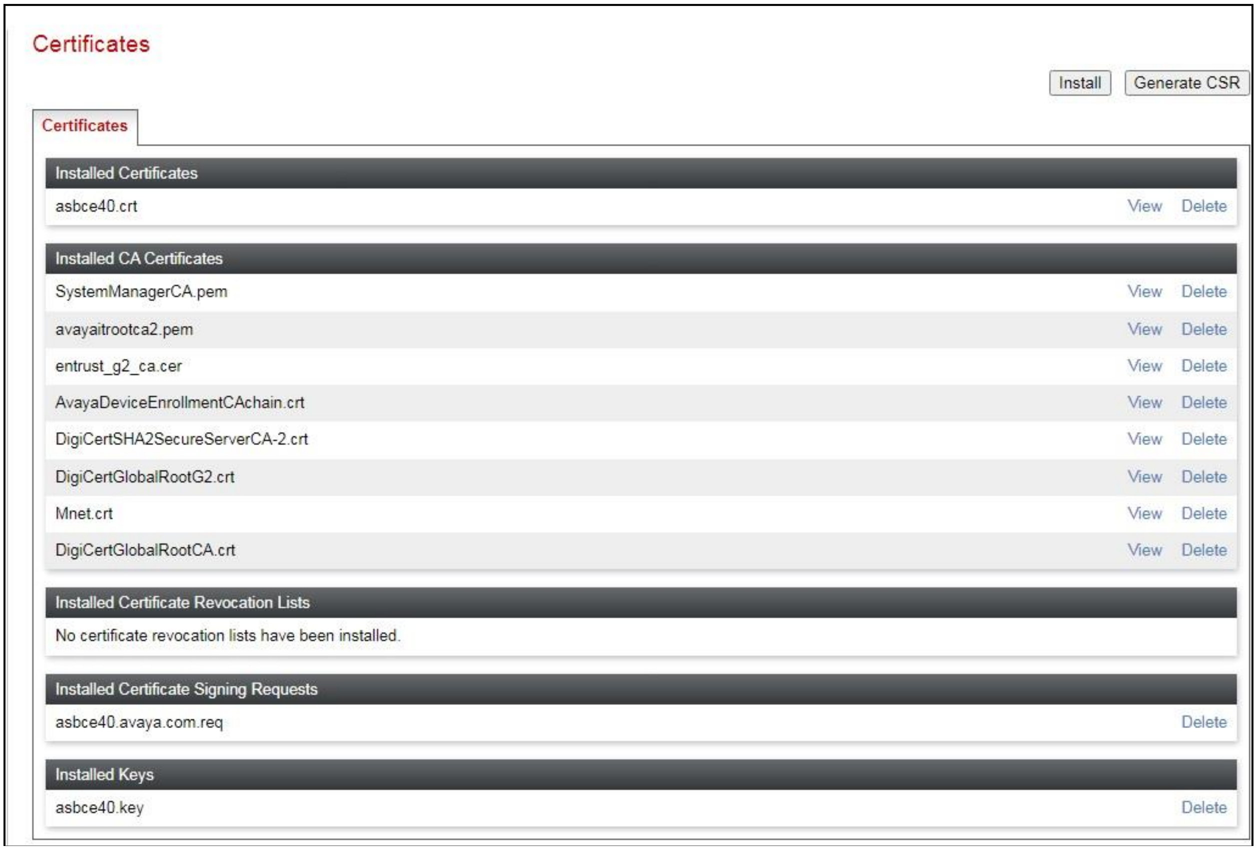
For the compliance test, TLS transport is used for signalling on the SIP trunk between IP Office and the Avaya SBC. Compliance testing was done using identity certificates signed by a local certificate authority. The generation and installation of these certificates are beyond the scope of these Application Notes.

The following procedures show how to view the certificates and configure the Client and Server profiles to support the TLS connection.

6.3.1. Certificates

To view the certificates currently installed on the Avaya SBC, navigate to **TLS Management → Certificates**:

- Verify that an Avaya SBC identity certificate (**asbce40.crt**) is present under **Installed Certificates**.
- Verify that certificate authority root certificate (**SystemManagerCA.pem**) is present under **Installed CA certificates**.
- Verify that private key associated with the identity certificate (**asbce40.key**) is present under **Installed Keys**.



Certificates

Installed Certificates		
asbce40.crt	View	Delete

Installed CA Certificates		
SystemManagerCA.pem	View	Delete
avayaitrootca2.pem	View	Delete
entrust_g2_ca.cer	View	Delete
AvayaDeviceEnrollmentCAchain.crt	View	Delete
DigiCertSHA2SecureServerCA-2.crt	View	Delete
DigiCertGlobalRootG2.crt	View	Delete
Mnet.crt	View	Delete
DigiCertGlobalRootCA.crt	View	Delete

Installed Certificate Revocation Lists

No certificate revocation lists have been installed.

Installed Certificate Signing Requests	
asbce40.avaya.com.req	Delete

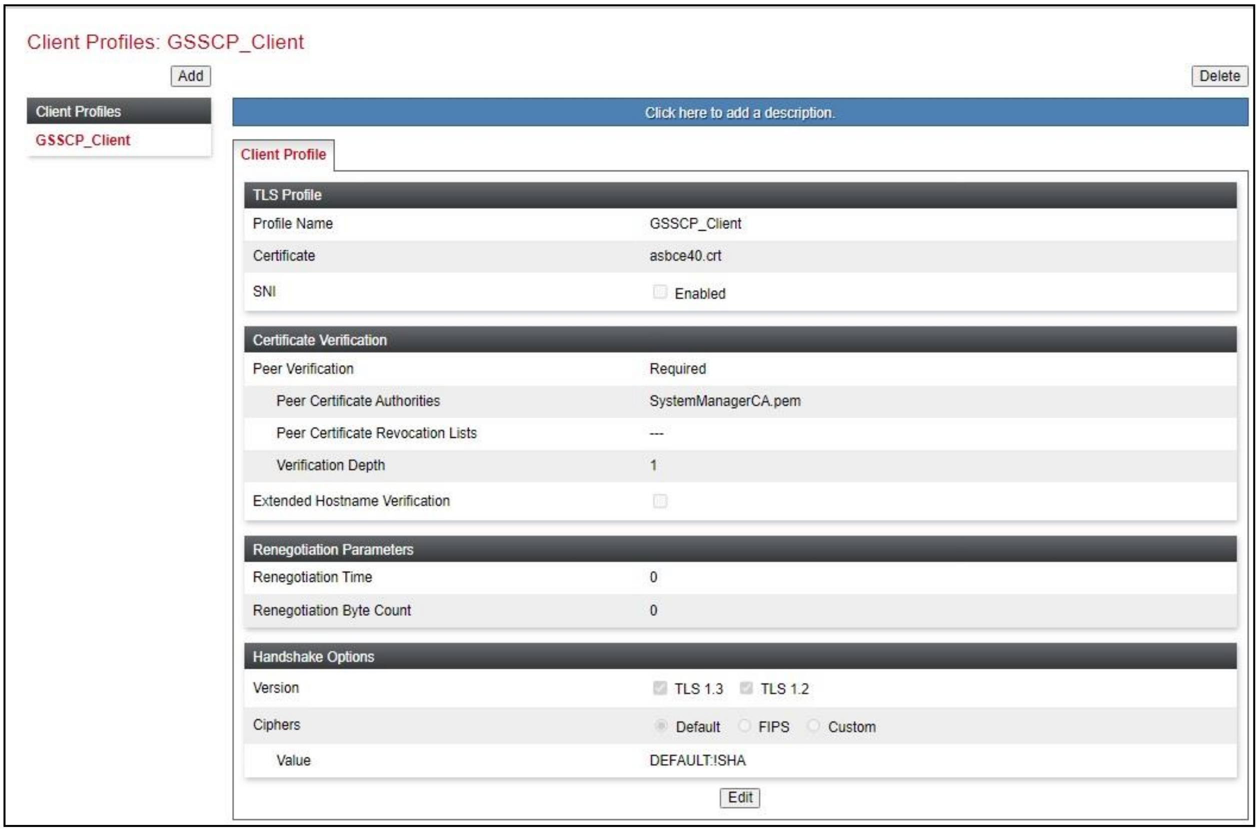
Installed Keys	
asbce40.key	Delete

6.3.2. Client Profile

To create a new client profile, navigate to **TLS Management → Client Profile** in the left pane and click **Add** (not shown).

- Set **Profile Name** to a descriptive name. **GSSCP_Client** was used in the compliance testing.
- Set **Certificate** to the identity certificate **asbce40.crt** used in the compliance testing.
- **Peer Verification** is automatically set to **Required**.
- Set **Peer Certificate Authorities** to the **SystemManagerCA.pem** identity certificate.
- Set **Verification Depth** to **1**.

Click **Next** to accept default values for the next screen and click **Finish** (not shown).


Client Profiles: GSSCP_Client
Add
Delete
Client Profiles
GSSCP_Client
Click here to add a description.
Client Profile
Edit

TLS Profile	
Profile Name	GSSCP_Client
Certificate	asbce40.crt
SNI	□ Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	□

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

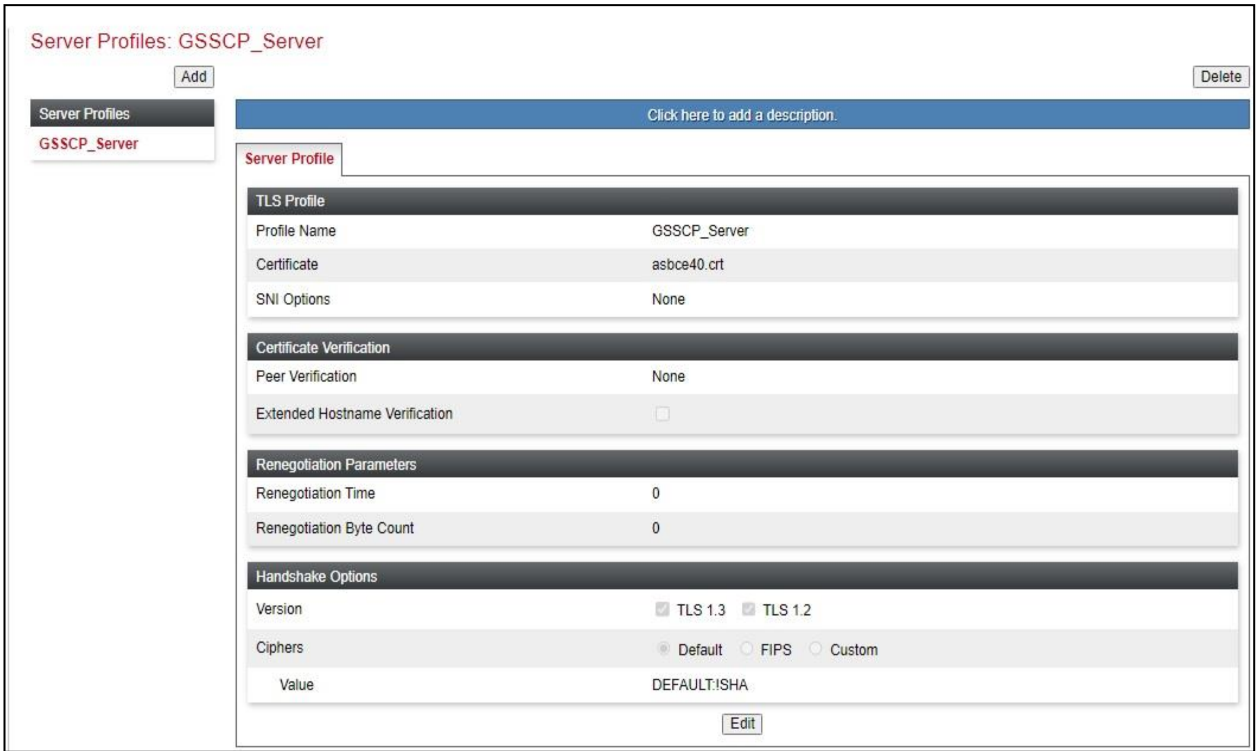
Handshake Options	
Version	☑ TLS 1.3 ☑ TLS 1.2
Ciphers	● Default ○ FIPS ○ Custom
Value	DEFAULT:!SHA

6.3.3. Server Profile

To create a new server profile, navigate to **TLS Management → Server Profile** in the left pane and click **Add** (not shown).

- Set **Profile Name** to a descriptive name. **GSSCP_Server** was used in the compliance testing
- Set **Certificate** to the identity certificate **asbce40.crt** used in the compliance testing.
- Set **Peer Verification** to **None**.

Click **Next** to accept default values for the next screen and click **Finish** (not shown).


Server Profiles: GSSCP_Server
Add
Delete
Server Profiles
GSSCP_Server
Click here to add a description.
Server Profile
Edit

TLS Profile	
Profile Name	GSSCP_Server
Certificate	asbce40.crt
SNI Options	None

Certificate Verification	
Peer Verification	None
Extended Hostname Verification	□

Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options	
Version	☑ TLS 1.3 ☑ TLS 1.2
Ciphers	● Default ○ FIPS ○ Custom
Value	DEFAULT:!SHA

6.4. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

6.4.1. Signalling Interfaces

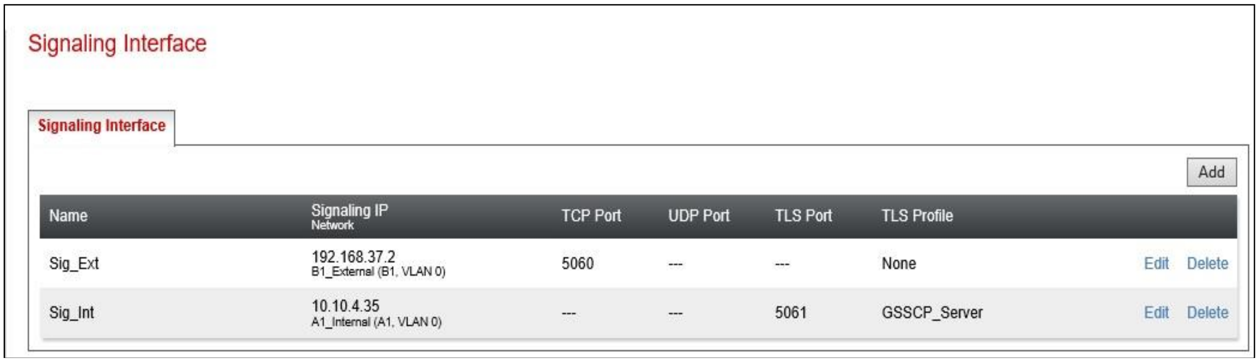
To define the signalling interfaces on the Avaya SBC, navigate to **Network & Flows → Signaling Interface** from the menu on the left-hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

To enter details of transport protocol and ports for the SIP signalling on the internal interface:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the interface.
- For **Signaling IP**, select the **A1_Internal** signalling interface IP addresses defined in **Section 6.2**.
- Select **TLS** port number, **5061** is used for IP Office.
- Select a **TLS Profile** defined in **Section 6.3.3** from the drop-down menu.
- Click **Finish**.

To enter details of transport protocol and ports for the SIP signalling on the external interface:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **IP Address**, select the **B1_external** signalling interface IP address defined in **Section 6.2**.
- Select **TCP** port number, **5060** is used for the Swisscom trunk.
- Click **Finish**.



Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Ext	192.168.37.2 B1_External (B1, VLAN 0)	5060	---	---	None	Edit Delete
Sig_Int	10.10.4.35 A1_Internal (A1, VLAN 0)	---	---	5061	GSSCP_Server	Edit Delete

6.4.2. Media Interfaces

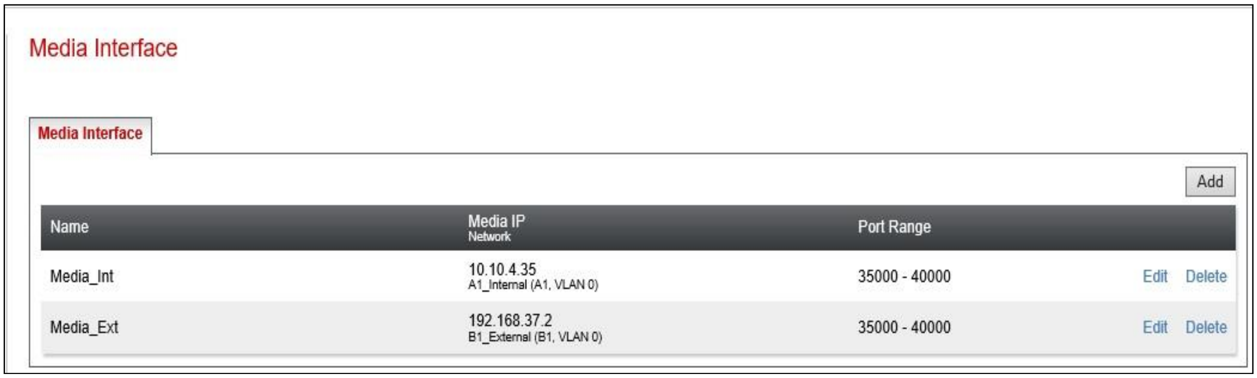
To define the media interfaces on the Avaya SBC, navigate to **Network & Flows → Media Interface** from the menu on the left-hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

To enter details of the media IP and RTP port range for the internal interface to be used in the server flow:

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **Media IP**, select the **A1_Internal** media interface IP address defined in **Section 6.2**.
- For **Port Range**, enter **35000-40000**.
- Click **Finish**.

To enter details of the media IP and RTP port range on the external interface to be used in the server flow.

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **Media IP**, select the **B1_External** media interface IP address defined in **Section 6.2**.
- Select **Port Range**, enter **35000-40000**.
- Click **Finish**.



Name	Media IP Network	Port Range		
Media_Int	10.10.4.35 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit	Delete
Media_Ext	192.168.37.2 B1_External (B1, VLAN 0)	35000 - 40000	Edit	Delete

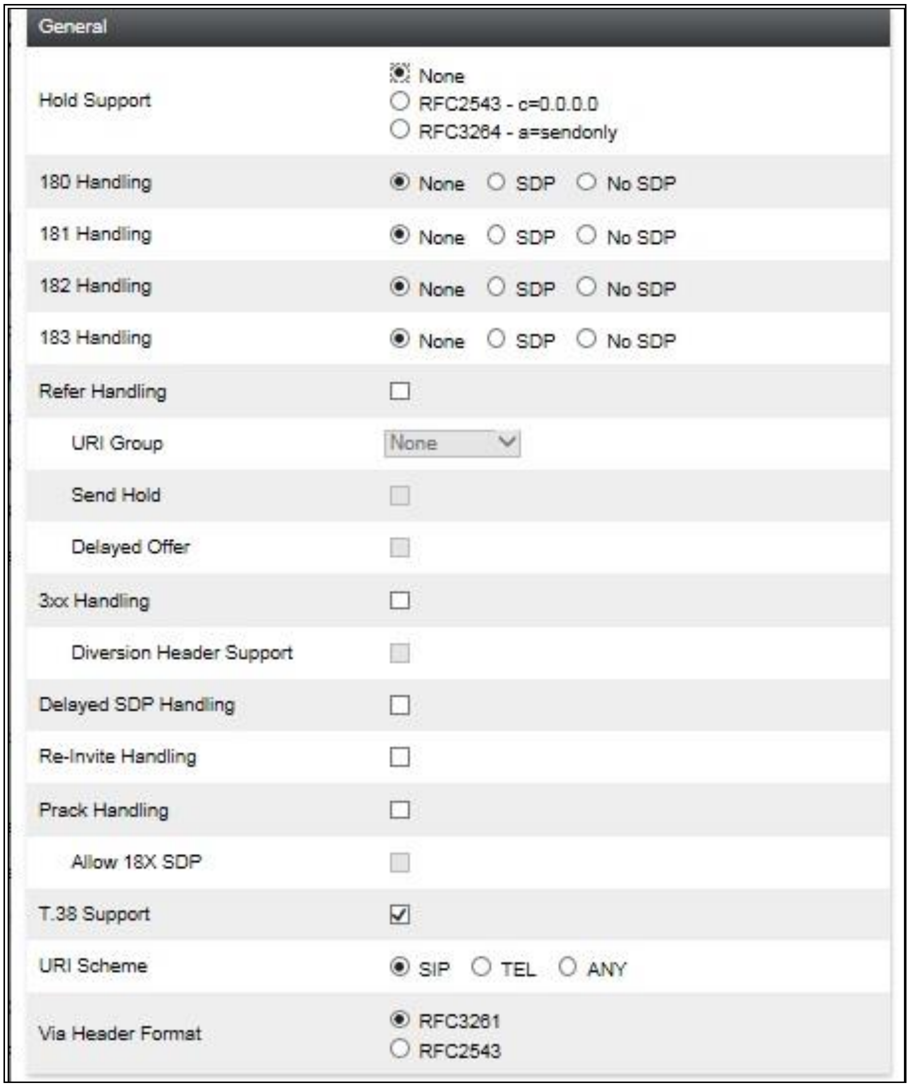
6.5. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBC. In this case, Swisscom is connected as the Trunk Server and the IP Office is connected as the Call Server.

6.5.1. Server Interworking Avaya

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Configuration Profiles → Server Interworking** and click on **Add**.

- Enter profile name such as Avaya and click **Next** (Not Shown).
- Check **Hold Support = None**.
- All other options on the **General** Tab can be left at default.



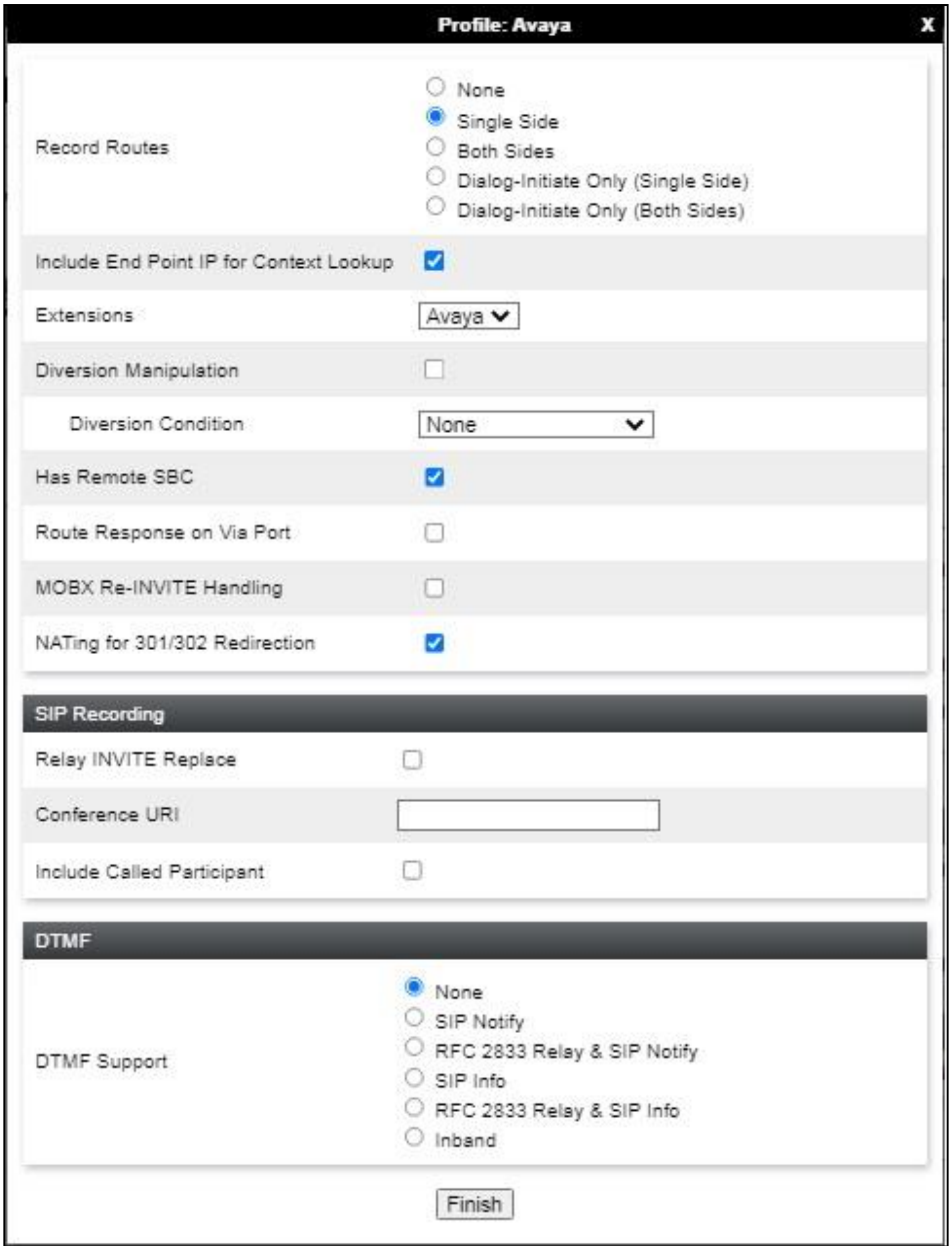
General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
Send Hold	□
Delayed Offer	□
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
Prack Handling	□
Allow 18X SDP	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

On the **Advanced** Tab:

- Check **Record Routes** = **Single Side**.
- Ensure **Extensions** = **Avaya**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.



Profile: Avaya

Record Routes	○ None ● Single Side ○ Both Sides ○ Dialog-Initiate Only (Single Side) ○ Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	☑
Extensions	Avaya
Diversion Manipulation	□
Diversion Condition	None
Has Remote SBC	☑
Route Response on Via Port	□
MOBX Re-INVITE Handling	□
NATing for 301/302 Redirection	☑

SIP Recording

Relay INVITE Replace	□
Conference URI	
Include Called Participant	□

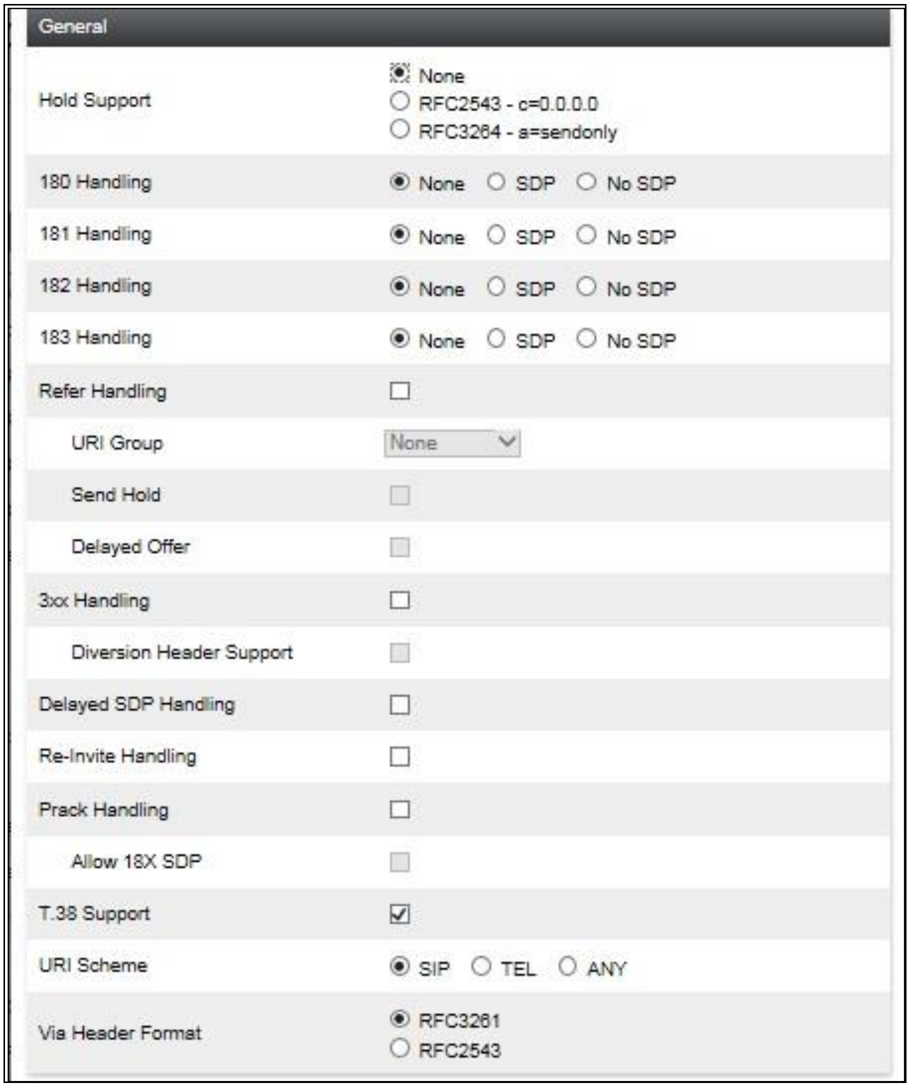
DTMF

DTMF Support	● None ○ SIP Notify ○ RFC 2833 Relay & SIP Notify ○ SIP Info ○ RFC 2833 Relay & SIP Info ○ Inband

6.5.2. Server Interworking – Swisscom

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Configuration Profiles → Server Interworking** and click on **Add**.

- Enter profile name such as Swisscom and click **Next** (Not Shown).
- Check **Hold Support = None**.
- All other options on the **General** Tab can be left at default.



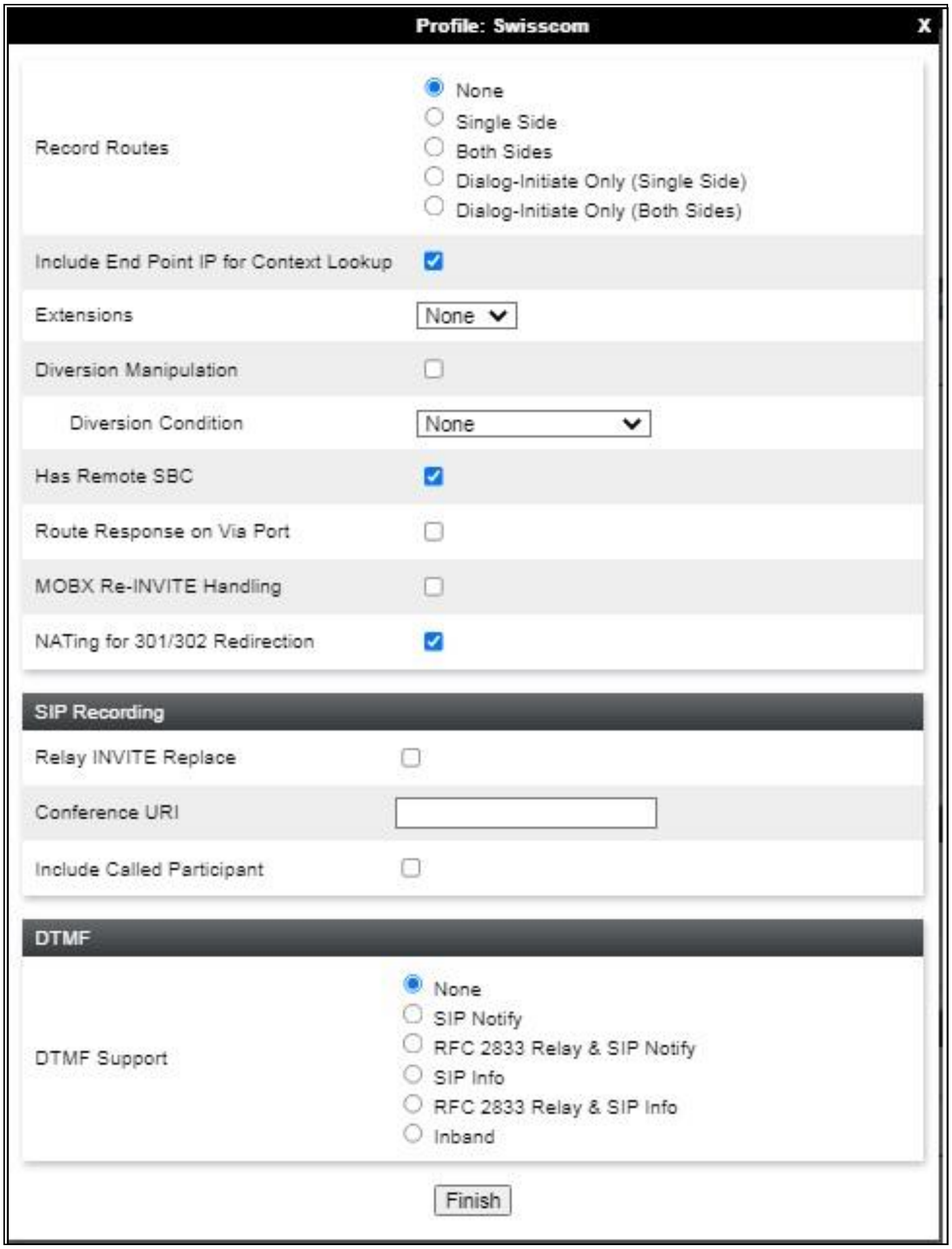
General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
Send Hold	□
Delayed Offer	□
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
Prack Handling	□
Allow 18X SDP	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

On the **Advanced** Tab:

- Check **Record Routes** = **None**.
- Ensure **Extensions** = **None**.
- Check **Has Remote SBC**.
- All other options on the **Advanced** Tab can be left at default.

Click **Finish**.



Profile: Swisscom X

Record Routes	● None ○ Single Side ○ Both Sides ○ Dialog-Initiate Only (Single Side) ○ Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	☑
Extensions	None
Diversion Manipulation	□
Diversion Condition	None
Has Remote SBC	☑
Route Response on Via Port	□
MOBX Re-INVITE Handling	□
NATing for 301/302 Redirection	☑

SIP Recording

Relay INVITE Replace	□
Conference URI	
Include Called Participant	□

DTMF

DTMF Support	● None ○ SIP Notify ○ RFC 2833 Relay & SIP Notify ○ SIP Info ○ RFC 2833 Relay & SIP Info ○ Inband

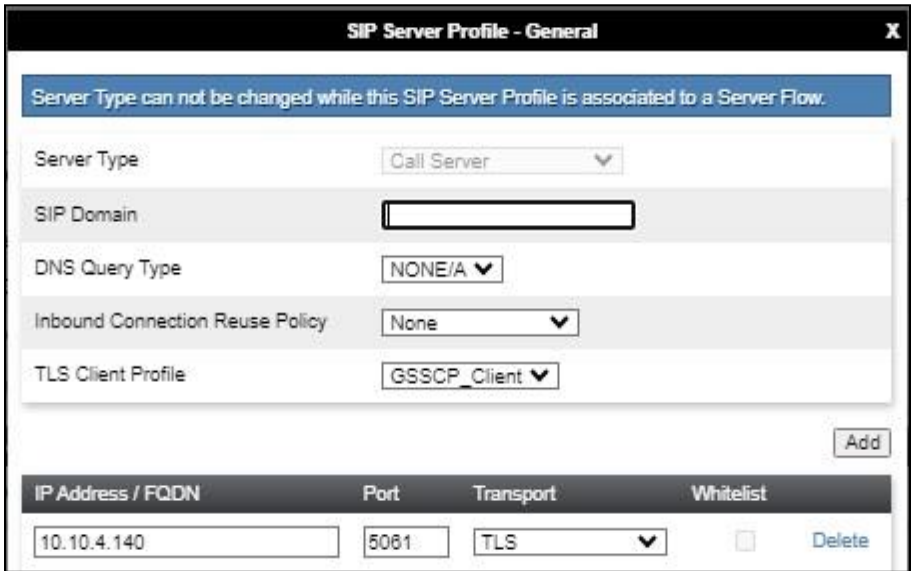
6.6. Define Servers

Servers are defined for each server connected to the Avaya SBC. In this case, Swisscom is connected as the Trunk Server and IP Office is connected as the Call Server.

6.6.1. Server Configuration – Avaya

From the left-hand menu select **Services → SIP Servers** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profiles** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Select **TLS Client Profile** to be **GSSCP_Client** as defined in **Section 6.3.2**.
- Enter **IP Address / FQDN** to **10.10.4.140** (IP Office IP Address).
- For **Port**, enter **5061**.
- For **Transport,** select **TLS**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.



SIP Server Profile - General

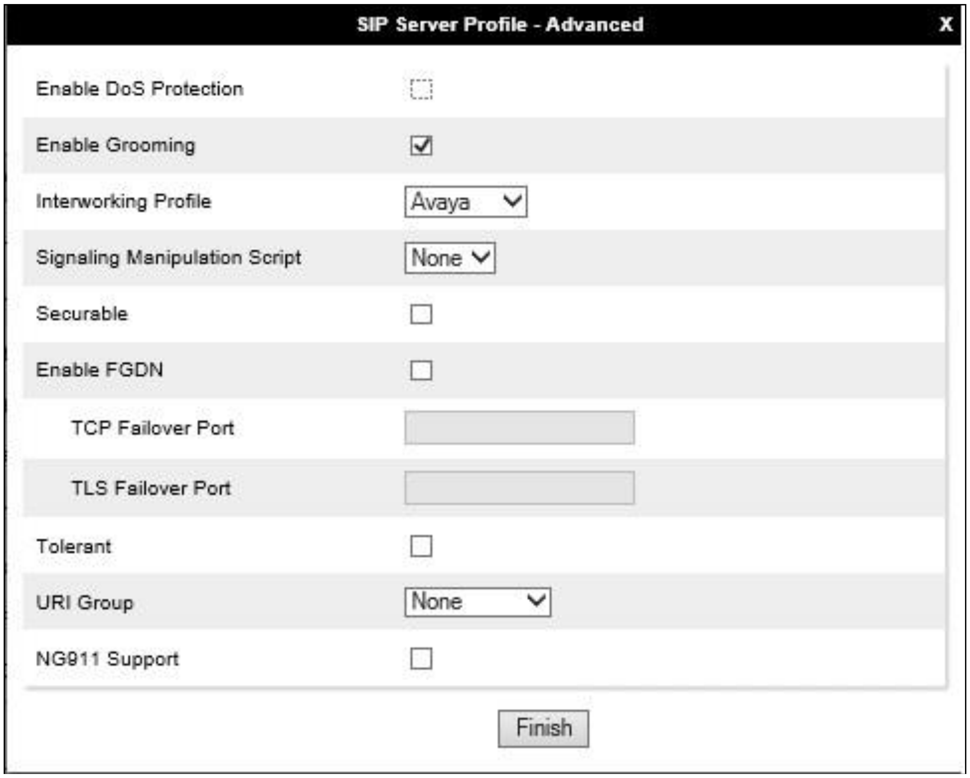
Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type	Call Server
SIP Domain	
DNS Query Type	NONE/A
Inbound Connection Reuse Policy	None
TLS Client Profile	GSSCP_Client

IP Address / FQDN	Port	Transport	Whitelist
10.10.4.140	5061	TLS	□

On the **Advanced** tab:

- Check **Enable Grooming**.
- Select **Avaya** for **Interworking Profile**.
- Click **Finish**.



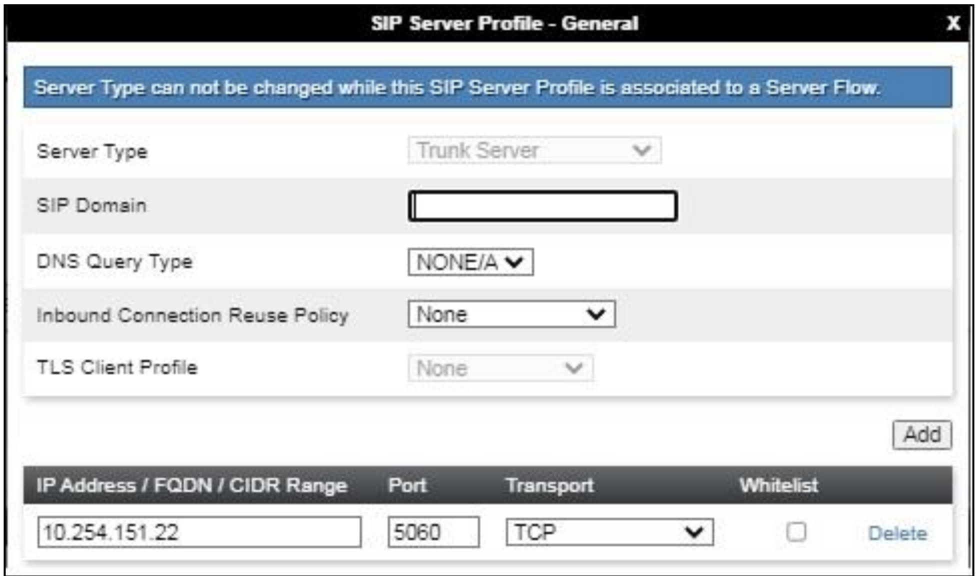
SIP Server Profile - Advanced

Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	Avaya
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
TCP Failover Port	
TLS Failover Port	
Tolerant	□
URI Group	None
NG911 Support	□

6.6.2. Server Configuration – Swisscom

To define the Swisscom Trunk Server, navigate to **Services → SIP Servers** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **10.254.151.22** (Swisscom SIP Network).
- For **Port**, enter **5060**.
- For **Transport,** select **TCP**.
- Click on **Next** (not shown).



SIP Server Profile - General

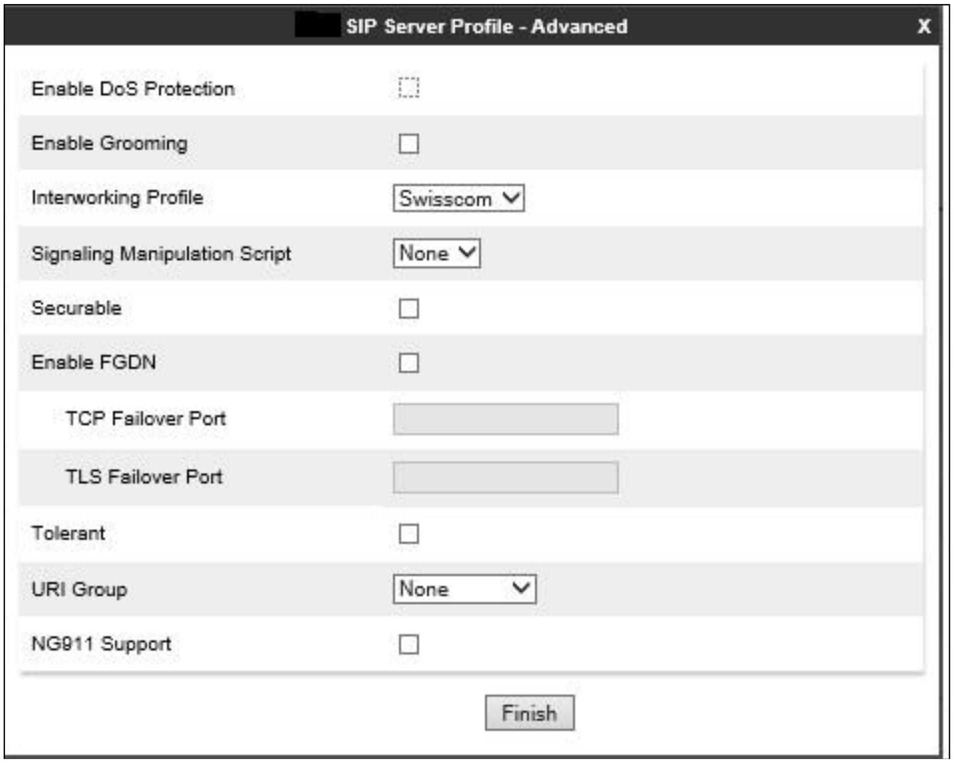
Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type	Trunk Server
SIP Domain	
DNS Query Type	NONE/A
Inbound Connection Reuse Policy	None
TLS Client Profile	None

IP Address / FQDN / CIDR Range	Port	Transport	Whitelist	
10.254.151.22	5060	TCP	□	Delete

On the Advanced tab:

- Enable **Grooming**.
- Select **Swisscom** for **Interworking Profile**.
- Click **Finish**.



[redacted] SIP Server Profile - Advanced X

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Swisscom
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
TCP Failover Port	
TLS Failover Port	
Tolerant	□
URI Group	None
NG911 Support	□

6.7. Routing

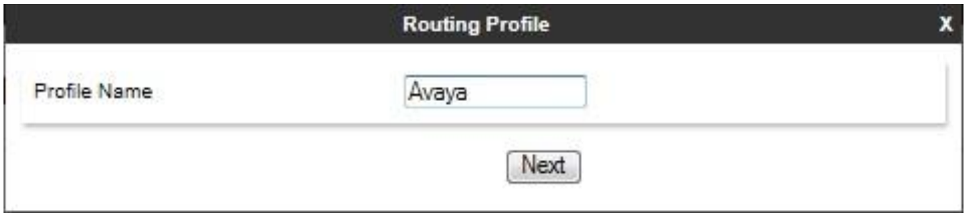
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Routing information is required for routing to IP Office on the internal side and Swisscom address on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

6.7.1. Routing – Avaya

Create a Routing Profile for IP Office.

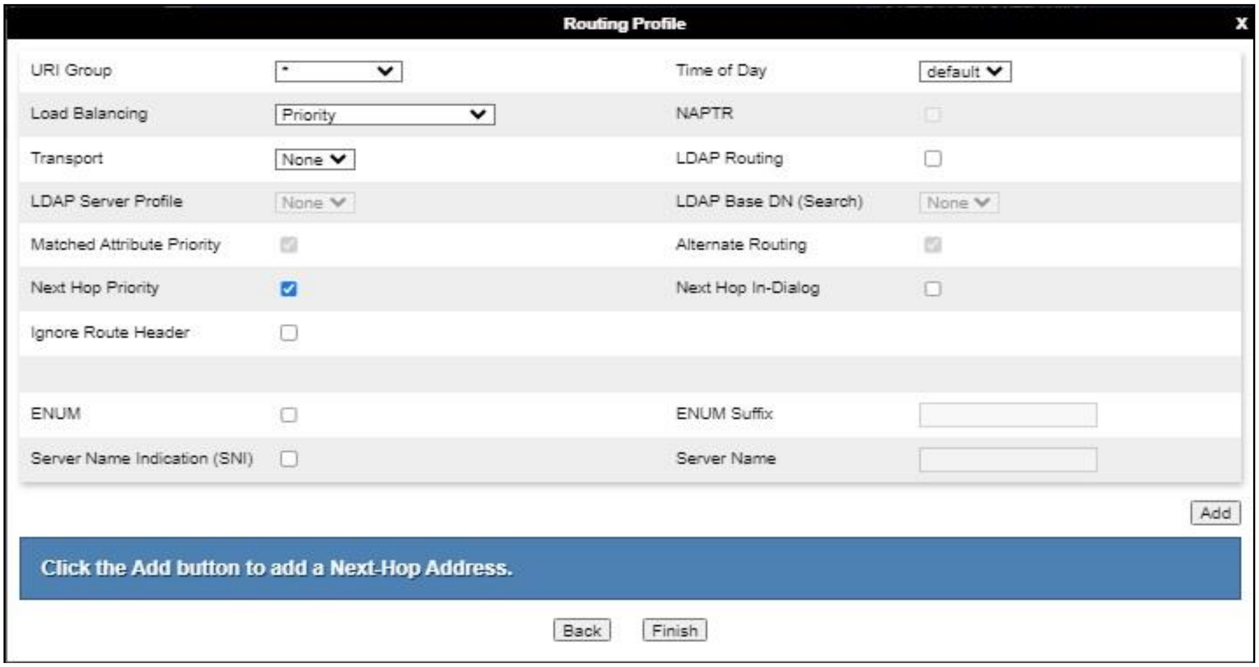
- Navigate to **Configuration Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.



Routing Profile

Profile Name	Avaya

The Routing Profile window will open. Use the default values displayed and click **Add**.



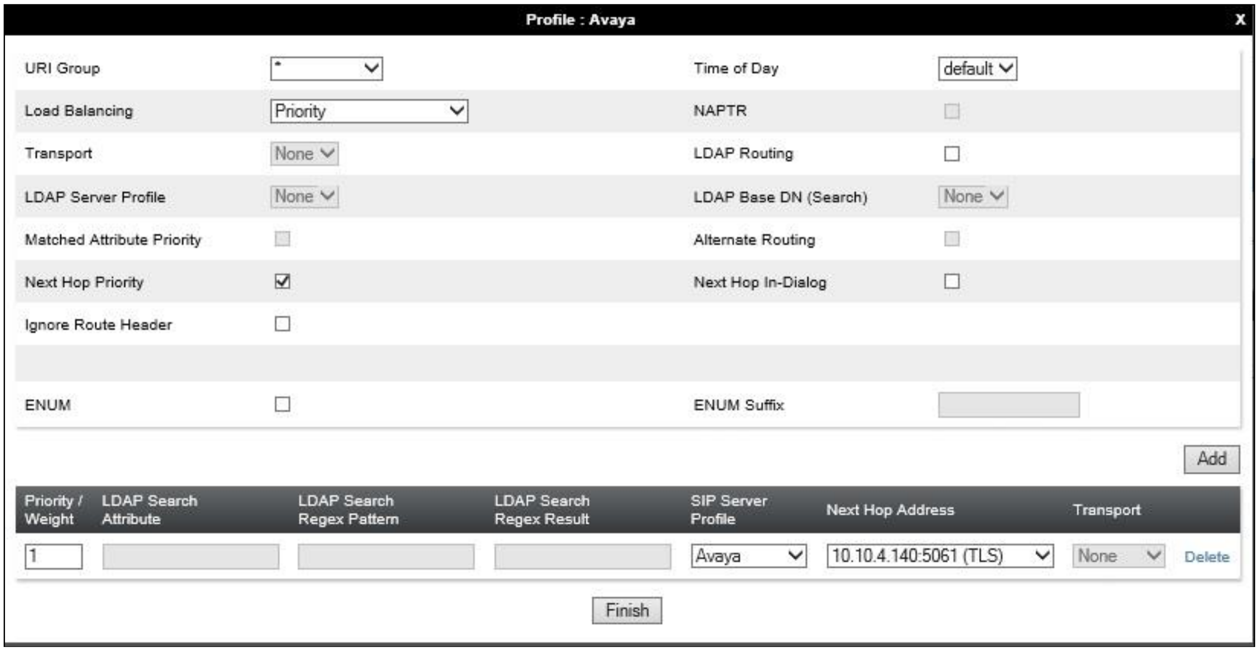
Routing Profile

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	☑	Alternate Routing	☑
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	
Server Name Indication (SNI)	□	Server Name	

Click the Add button to add a Next-Hop Address.

On the **Next Hop Address** window, set the following:

- **Priority/Weight** = **1**.
- **SIP Server Profile** = **Avaya** (**Section 6.6.1**) from drop down menu.
- **Next Hop Address** = Select **10.10.4.140:5061 (TLS)** from drop down menu.
- Click **Finish**.



Profile : Avaya

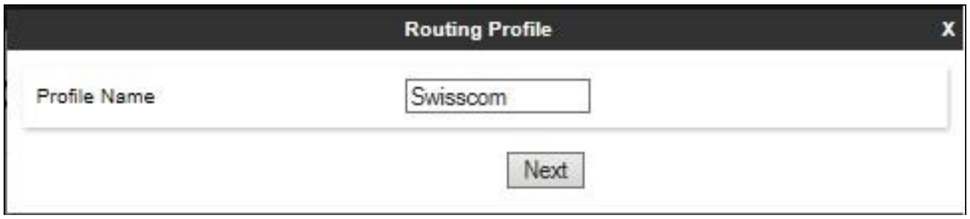
URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Avaya	10.10.4.140:5061 (TLS)	None	Delete

6.7.2. Routing – Swisscom

Create a Routing Profile for Swisscom SIP network.

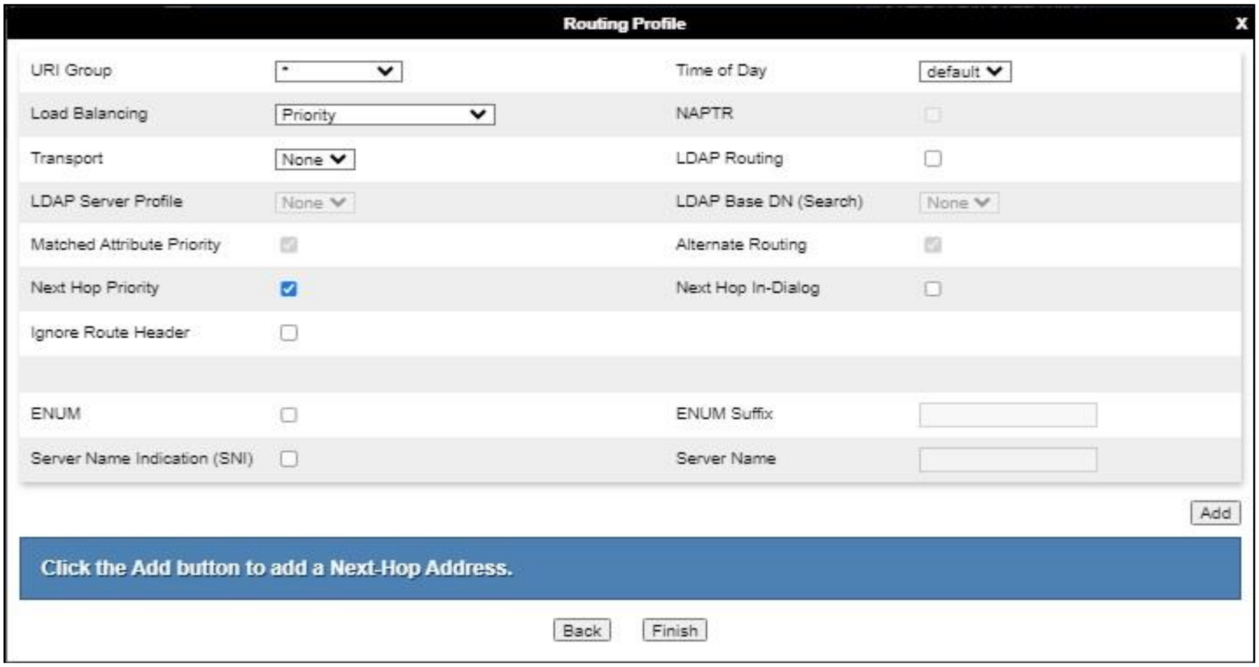
- Navigate to **Configuration Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.



Routing Profile

Profile Name: Swisscom

The Routing Profile window will open. Use the default values displayed and click **Add**.

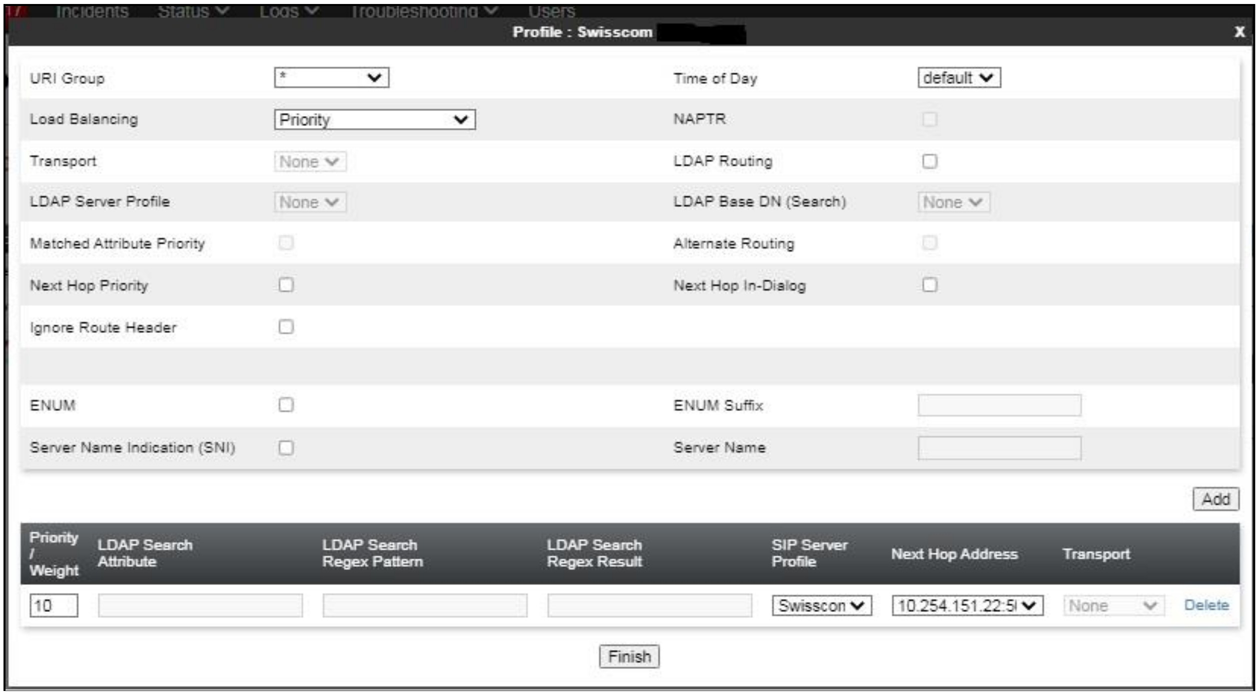


URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	☑	Alternate Routing	☑
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	
Server Name Indication (SNI)	□	Server Name	

Click the Add button to add a Next-Hop Address.

On the **Next Hop Address** window, set the following:

- **Priority/Weight** = **1**.
- **SIP Server Profile** = **Swisscom** (**Section 6.6.2**) from drop down menu.
- **Next Hop Address** = Select **10.254.151.22 (TCP)** from drop down menu.
- Click **Finish**.



URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	□	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	
Server Name Indication (SNI)	□	Server Name	

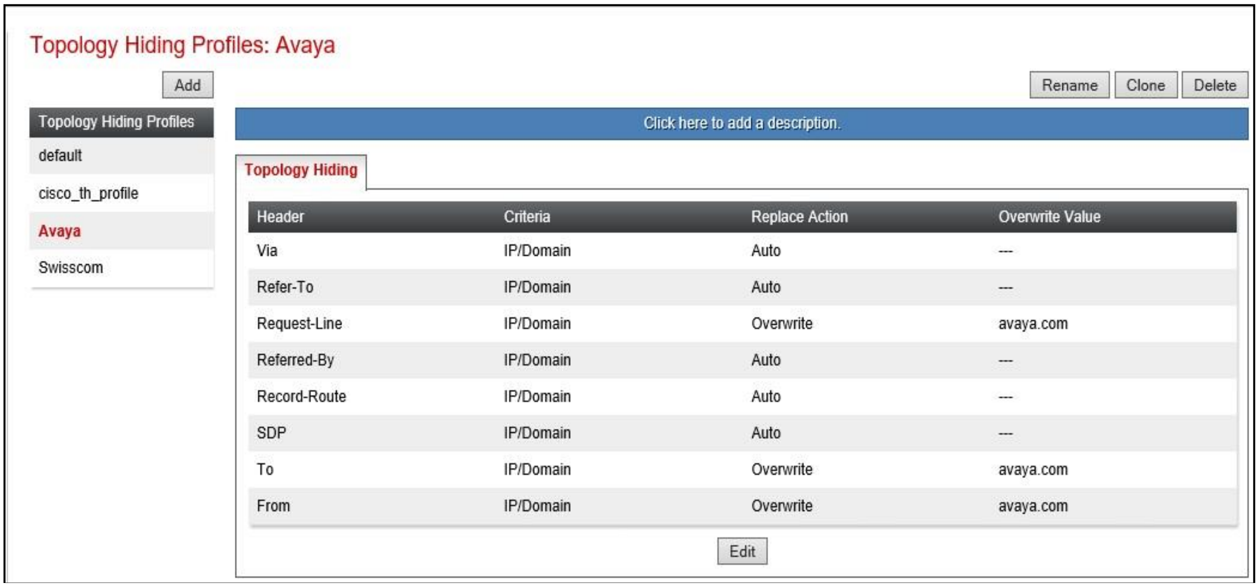
Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
10				Swisscon	10.254.151.22:5(	None	Delete

6.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise. In some cases where Topology Hiding cannot be applied, in particular the Contact header, IP addresses are translated to the Avaya SBC external addresses using NAT.

To define Topology Hiding for IP Office, navigate to **Configuration Profiles → Topology Hiding** from menu on the left-hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown).

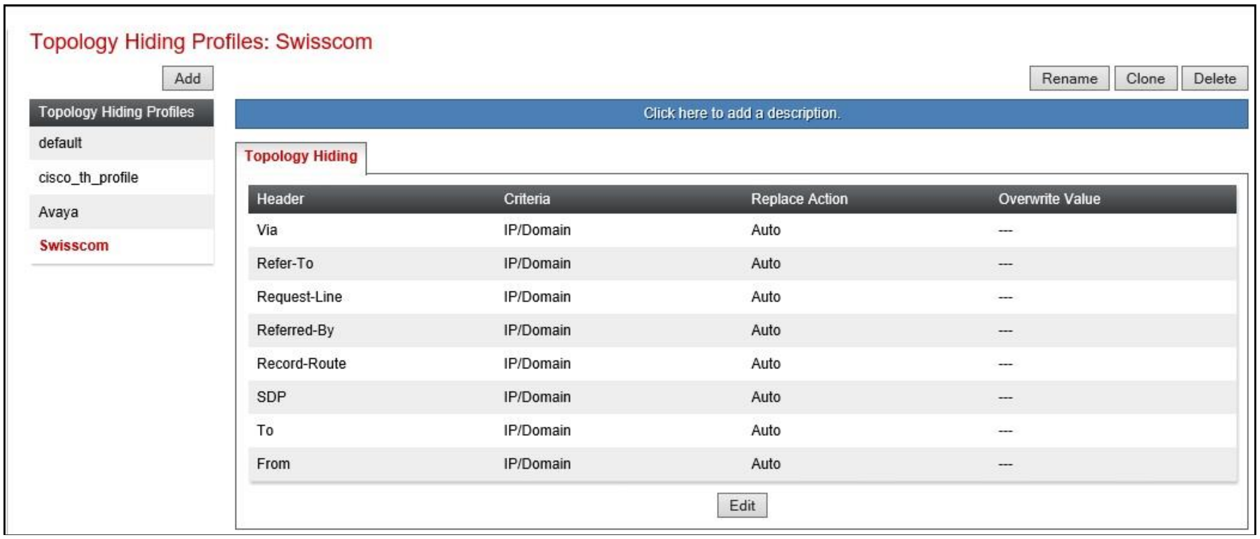


Topology Hiding Profiles: Avaya

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	avaya.com
Referred-By	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	avaya.com
From	IP/Domain	Overwrite	avaya.com

To define Topology Hiding for Swisscom, navigate to **Configuration Profiles → Topology Hiding** from the menu on the left-hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for Swisscom and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Auto** under **Replace Action**.
- Click **Finish** (not shown).



Topology Hiding Profiles: Swisscom

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---

6.9. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signalling, Security, etc.

In the reference configuration, only new Media Rules were defined. All other rules under Domain Policies, linked together on End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

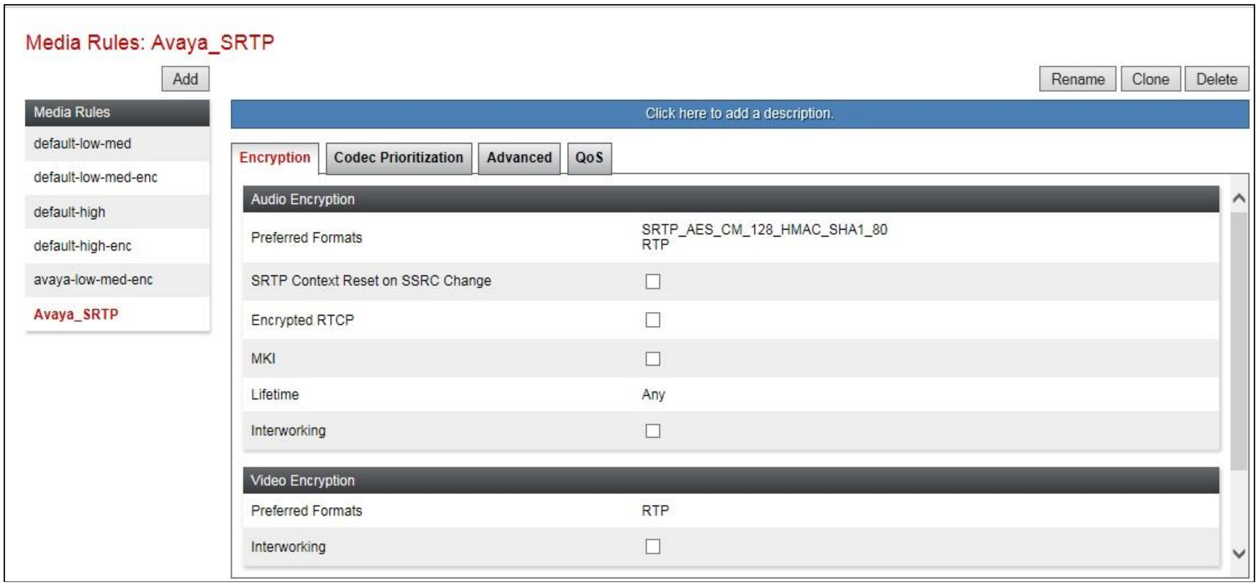
6.9.1. Media Rules

A media rule defines the processing to be applied to the selected media. For the compliance test, media rules were created for both Avaya IP Office and Swisscom to use SRTP.

To define the Media Rule for IP Office, navigate to **Domain Policies →Media Rules** in the main menu on the left-hand side. Click on **Add** and enter details in the Media Rule pop-up box (not shown)

- In the **Rule Name** field enter a descriptive name such as **Avaya_SRTP**.
- Set **Preferred Format #1** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Set **Preferred Format #2** to **RTP**.
- Uncheck **Encrypted RTCP**.
- Check **Capability Negotiation** under **Miscellaneous** (not shown).

Default values were used for all other fields. Click **Finish** (not shown).



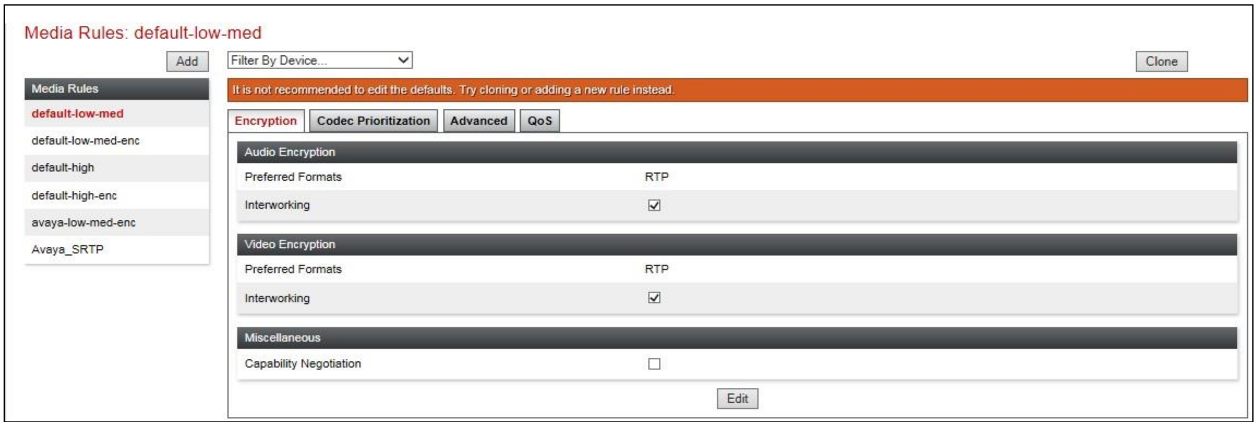
Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
SRTP Context Reset on SSRC Change	□
Encrypted RTCP	□
MKI	□
Lifetime	Any
Interworking	□

Video Encryption

Preferred Formats	RTP
Interworking	□

For the compliance test, the default media rule **default-low-med** was used for Swisscom.


Media Rules: default-low-med

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Audio Encryption	
Preferred Formats	RTP
Interworking	☑

Video Encryption	
Preferred Formats	RTP
Interworking	☑

Miscellaneous	
Capability Negotiation	□

6.10. End Point Policy Groups

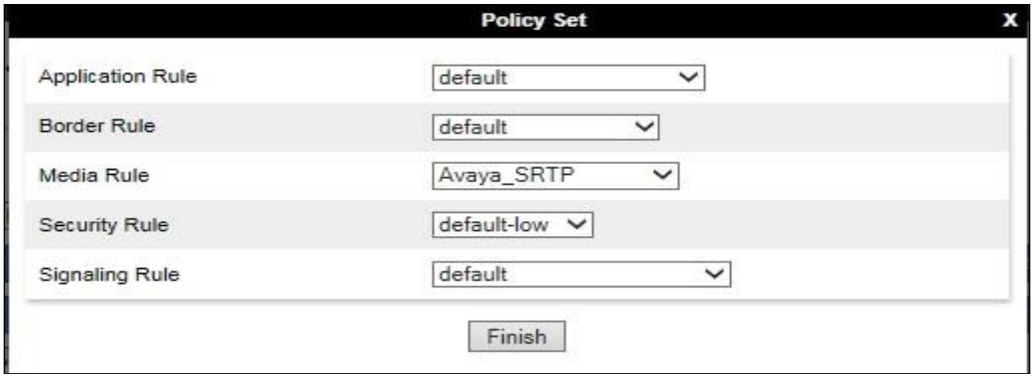
An end point policy group is a set of policies that will be applied to traffic between the Avaya SBC and a signalling endpoint (connected server). Thus, one end point policy group must be created for Avaya IP Office and another for the Swisscom SIP trunk. The end point policy group is applied to the traffic as part of the end point flow defined in **Section 6.11**.

6.10.1. End Point Policy Group – Avaya IP Office

To define an End Point policy for IP Office, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left-hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name, in this case **Avaya**, and click **Next** (not shown).
- Leave the **Application Rule**, **Border Rule**, **Security Rule** and **Signalling Rule** fields at their default values.
- In the **Media Rule** drop down menu, select the recently added Media Rule called **Avaya_SRTP**.

Click **Finish**.


Policy Set

Application Rule	default
Border Rule	default
Media Rule	Avaya_SRTP
Security Rule	default-low
Signaling Rule	default

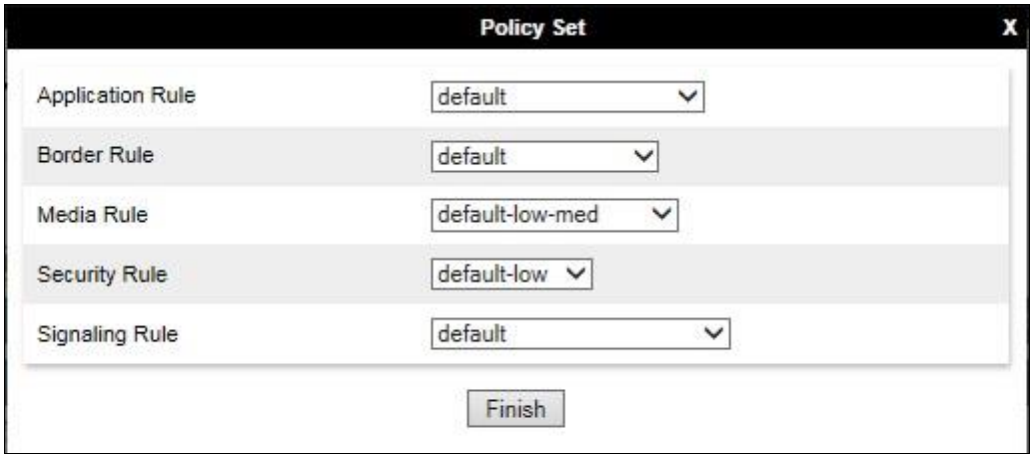
6.10.2. End Point Policy Group – Swisscom

For the compliance test, the end point policy group **Swisscom** was created for the Swisscom SIP trunk. Default values were used for each of the rules which comprise the group.

In the **Group Name** field enter a descriptive name, in this case **Swisscom** and click **Next** (not shown).

- Leave the **Application Rule**, **Border Rule**, **Media Rule**, **Security Rule** and **Signaling Rule** fields at their default values.

Click **Finish**.

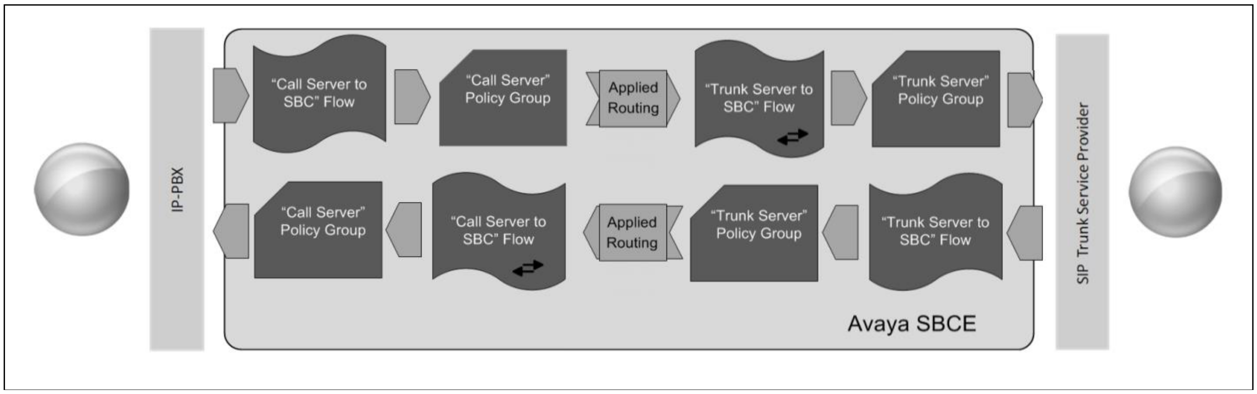


Policy Set

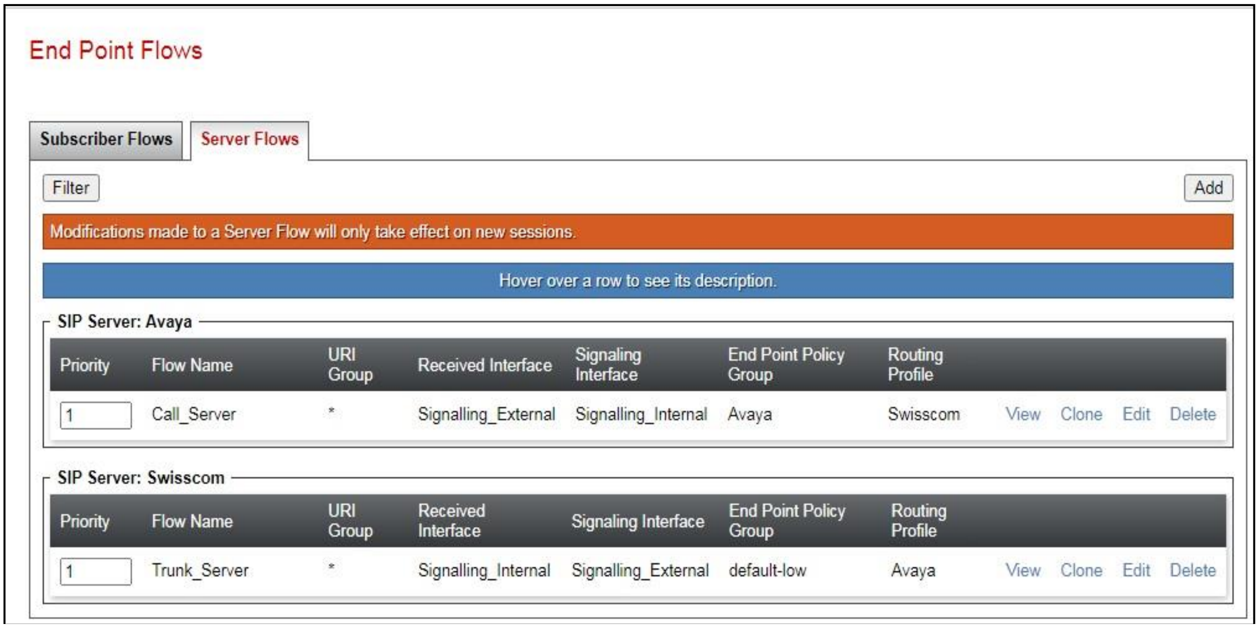
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default

6.11. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from IP Office to Swisscom's SIP Trunk and incoming flows from Swisscom's SIP Trunk to IP Office. The following screen illustrates the flow through the Avaya SBC to secure a SIP Trunk call.


IP-PBX
"Call Server to SBC" Flow
"Call Server" Policy Group
Applied Routing
"Trunk Server to SBC" Flow
"Trunk Server" Policy Group
"Call Server" Policy Group
"Call Server to SBC" Flow
Applied Routing
"Trunk Server" Policy Group
"Trunk Server to SBC" Flow
Avaya SBCE
SIP Trunk Service Provider

This configuration ties all the previously entered information together so that calls can be routed from IP Office to Swisscom SIP Trunk and vice versa. The following screenshot shows all configured flows.



End Point Flows

Modifications made to a Server Flow will only take effect on new sessions.

Hover over a row to see its description.

SIP Server: Avaya

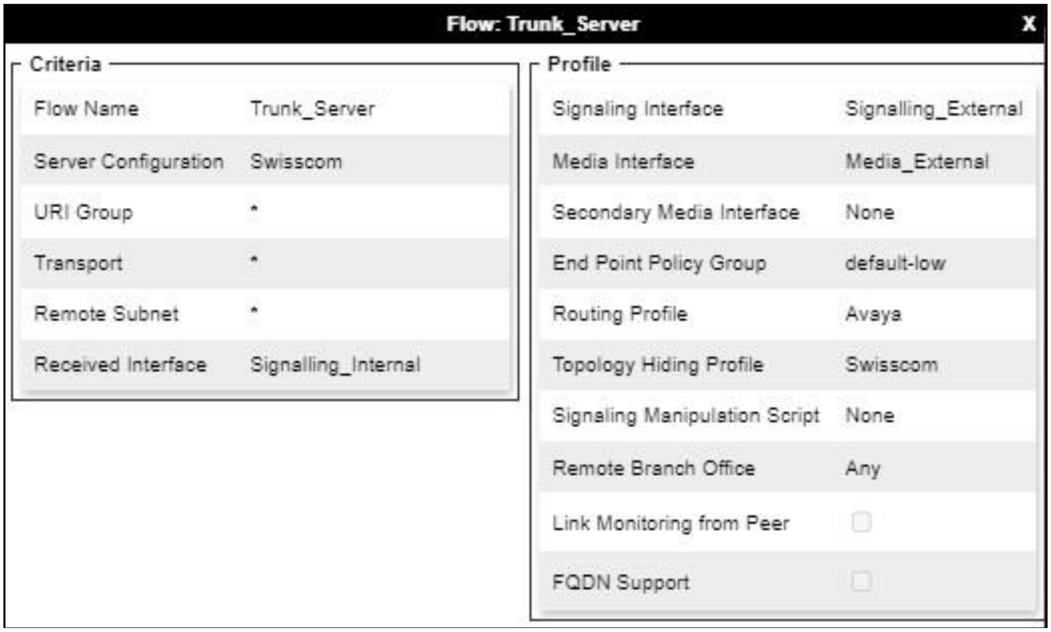
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Call_Server	*	Signalling_External	Signalling_Internal	Avaya	Swisscom	View	Clone	Edit	Delete

SIP Server: Swisscom

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk_Server	*	Signalling_Internal	Signalling_External	default-low	Avaya	View	Clone	Edit	Delete

To define a Server Flow for the Swisscom SIP Trunk, navigate to **Network & Flows → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Swisscom SIP Trunk, in the test environment **Trunk_Server** was used.
- In the **Server Configuration** drop-down menu, select the Swisscom server configuration defined in **Section 6.6.2**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 6.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 6.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **default-low**.
- In the **Routing Profile** drop-down menu, select the routing profile of the IP Office defined in **Section 6.7.1**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Swisscom SIP Trunk defined in **Section 6.8** and click **Finish** (not shown).



Flow: Trunk_Server

Criteria

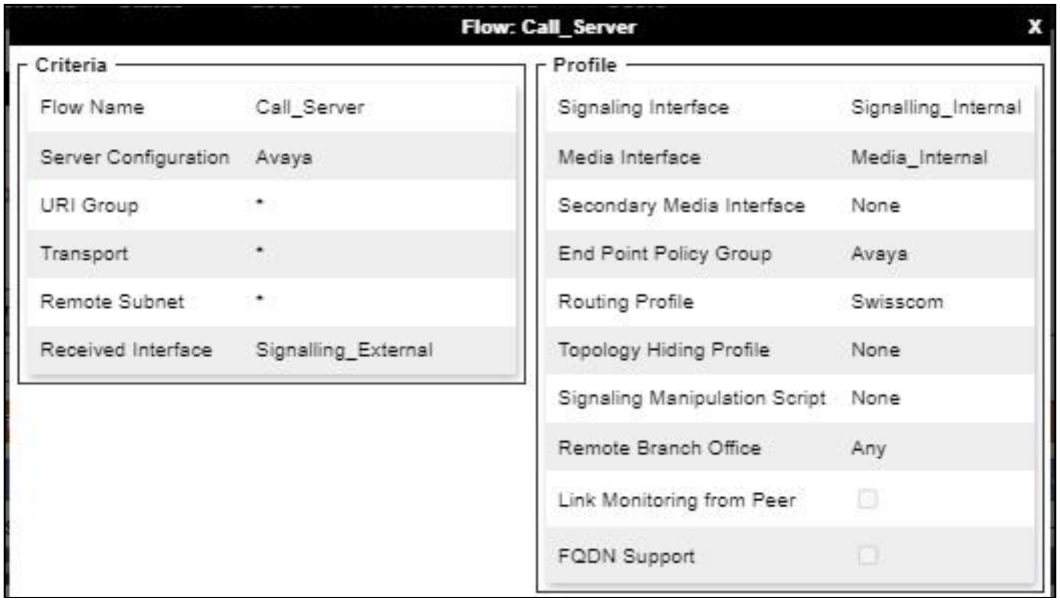
Flow Name	Trunk_Server
Server Configuration	Swisscom
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Signalling_Internal

Profile

Signaling Interface	Signalling_External
Media Interface	Media_External
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	Swisscom
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□
FQDN Support	□

To define an incoming server flow for IP Office from the Swisscom network, navigate to **Network & Flows → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for IP Office, in the test environment **Call_Server** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for IP Office defined in **Section 6.6.1**.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 6.4.1**.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 6.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 6.4.2**.
- Set the **End Point Policy Group** to the endpoint policy group **Avaya**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Swisscom SIP Trunk defined in **Section 6.7.2**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of IP Office defined in **Section 6.8** and click **Finish** (not shown).



Flow: Call_Server

Criteria

Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Signalling_External

Profile

Signaling Interface	Signalling_Internal
Media Interface	Media_Internal
Secondary Media Interface	None
End Point Policy Group	Avaya
Routing Profile	Swisscom
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□
FQDN Support	□

7. Swisscom SIP Trunk Configuration

The configuration of the Swisscom equipment used to support Swisscom's SIP trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on Swisscom equipment and system configuration please contact an authorized Swisscom representative as per **Section 2.3**.

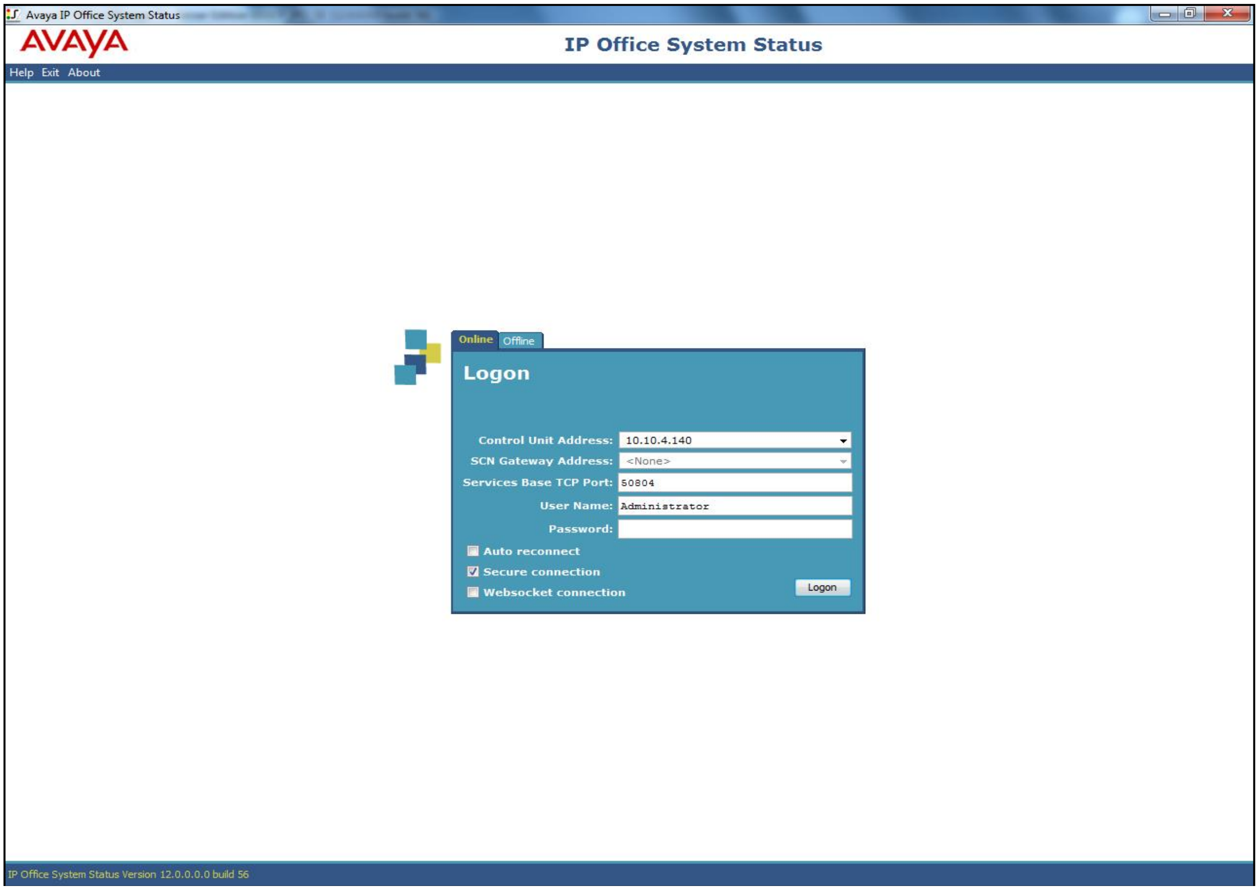
8. Verification Steps

This section includes steps that can be used to verify that the configuration has been done correctly.

8.1. SIP Trunk status

The status of the SIP trunk can be verified by opening the System Status application. This is found on the PC where IP Office Manager is installed in PC programs under **Start →All Programs →IP Office →System Status** (not shown).

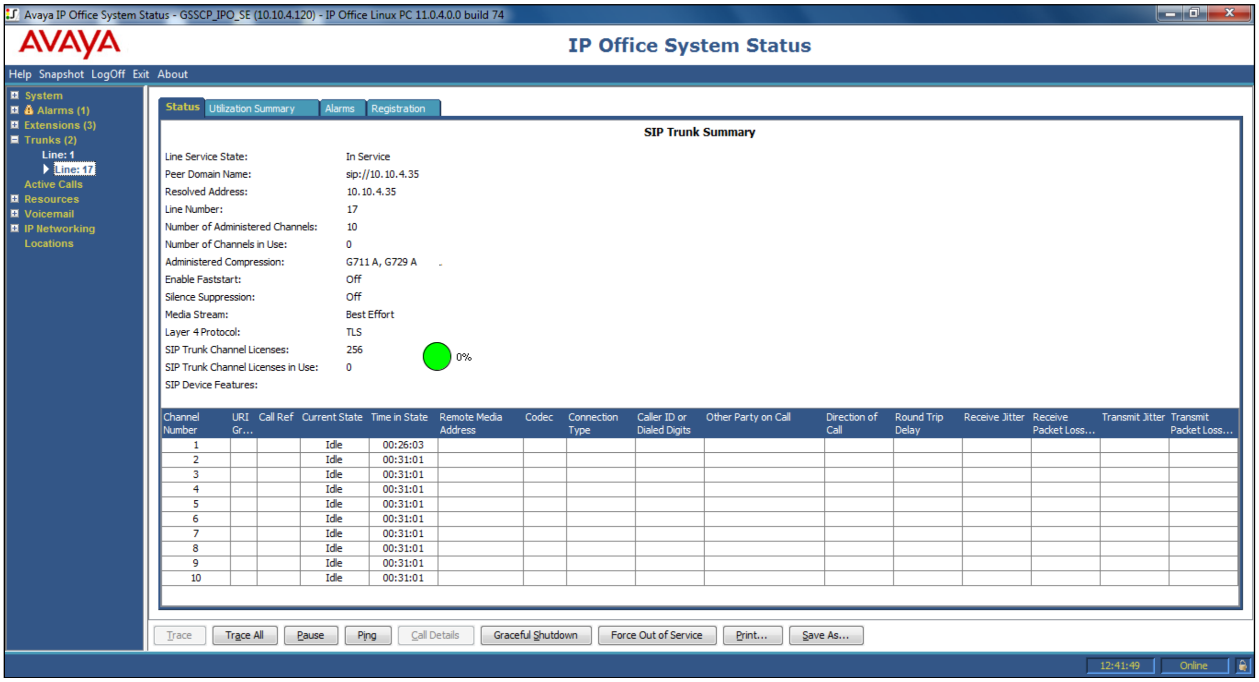
Log in to IP Office System Status at the prompt using the **Control Unit IP Address** for the IP Office. The **Username** and **Password** are the same as those used for IP Office Manager.



Control Unit Address: 10.10.4.140
SCN Gateway Address: <None>
Services Base TCP Port: 50804
User Name: Administrator
Password:
□ Auto reconnect
☑ Secure connection
□ Websocket connection

IP Office System Status Version 12.0.0.0.0 build 56

From the left-hand menu expand **Trunks** and choose the SIP trunk (**17** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational.



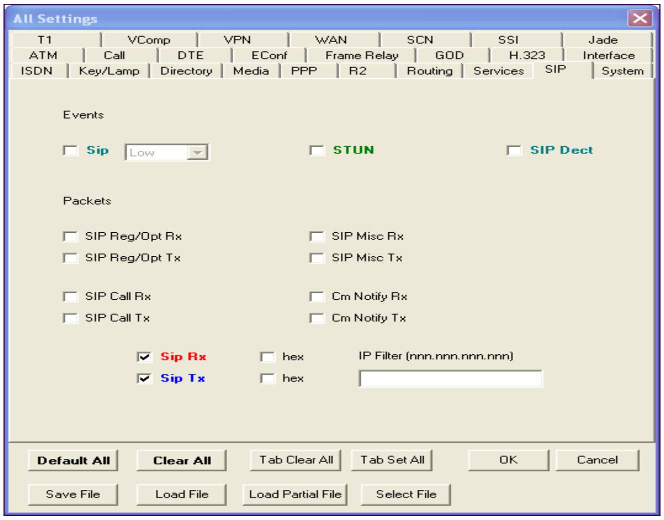
SIP Trunk Summary

Line Service State:	In Service
Peer Domain Name:	sip://10.10.4.35
Resolved Address:	10.10.4.35
Line Number:	17
Number of Administered Channels:	10
Number of Channels in Use:	0
Administered Compression:	G711 A, G729 A
Enable Faststart:	Off
Silence Suppression:	Off
Media Stream:	Best Effort
Layer 4 Protocol:	TLS
SIP Trunk Channel Licenses:	256 🟢 0%
SIP Trunk Channel Licenses in Use:	0
SIP Device Features:	

Channel Number	URI Gr...	Call Ref	Current State	Time in State	Remote Media Address	Codec	Connection Type	Caller ID or Dialed Digits	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet Loss...	Transmit Jitter	Transmit Packet Loss...
1			Idle	00:26:03											
2			Idle	00:31:01											
3			Idle	00:31:01											
4			Idle	00:31:01											
5			Idle	00:31:01											
6			Idle	00:31:01											
7			Idle	00:31:01											
8			Idle	00:31:01											
9			Idle	00:31:01											
10			Idle	00:31:01											

8.1.1. Monitor

The Monitor application can also be used to monitor and troubleshoot IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select the button that is third from the right in the screen below, or select **Filters →Trace Options**. The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, the **SIP Rx** and **SIP Tx** boxes are checked. All SIP messages will appear in the trace with the color blue. To customize the color, right-click on **SIP Rx** or **SIP Tx** and select the desired color.



Events

□ Sip [Low] □ STUN □ SIP Dect

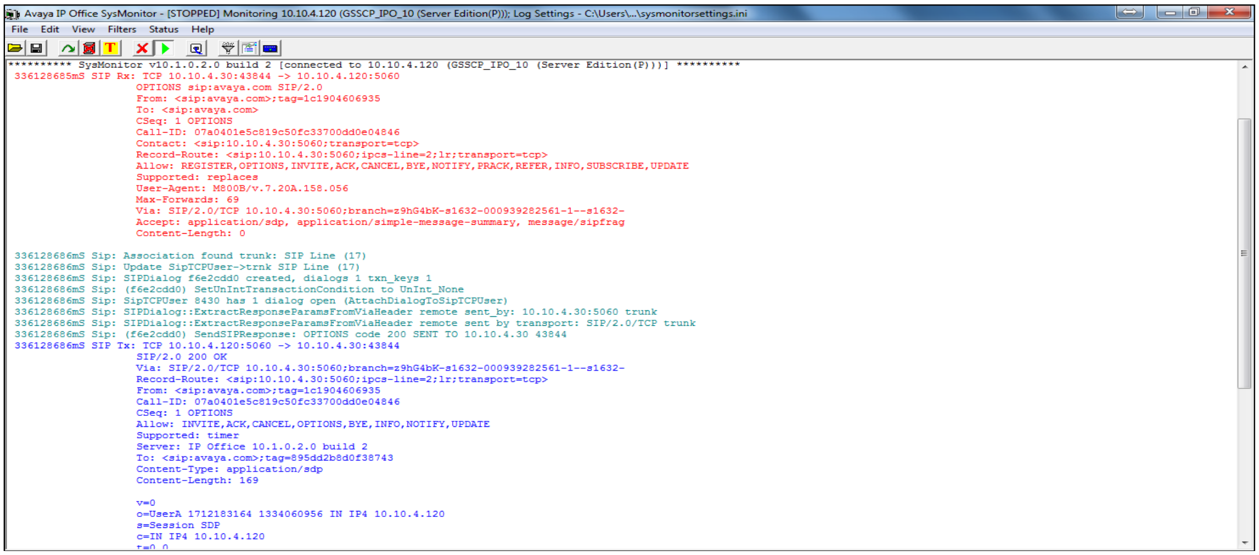
Packets

□ SIP Reg/Opt Rx □ SIP Misc Rx
□ SIP Reg/Opt Tx □ SIP Misc Tx

□ SIP Call Rx □ Cm Notify Rx
□ SIP Call Tx □ Cm Notify Tx

☑ Sip Rx □ hex IP Filter (nnn.nnn.nnn.nnn)
☑ Sip Tx □ hex

As an example, the following shows a portion of the monitoring window of OPTIONs being sent between IP Office and the Service Provider.


Avaya IP Office SysMonitor - [STOPPED] Monitoring 10.10.4.120 (GSSCP_IPO_10 (Server Edition(P))); Log Settings - C:\Users\...\sysmonitorsettings.ini
File
Edit
View
Filters
Status
Help

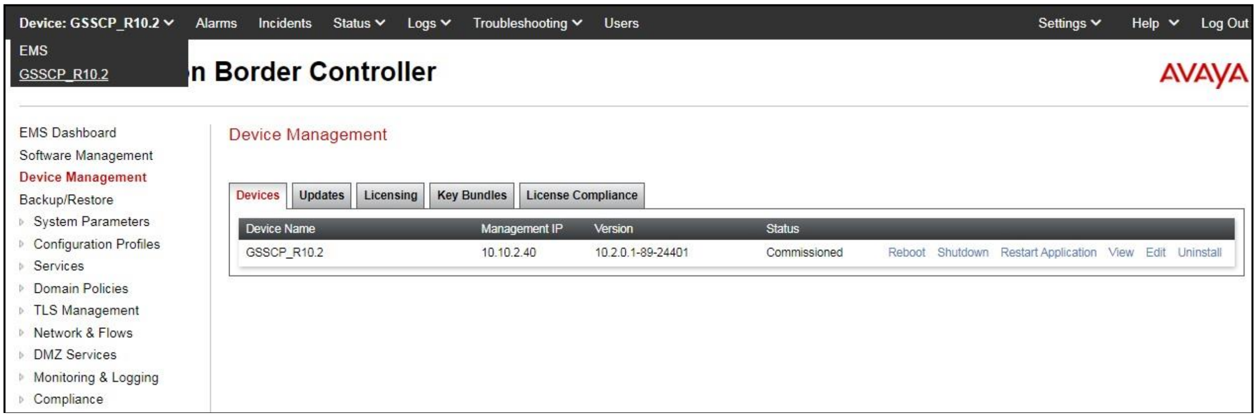
```
********** SysMonitor v10.1.0.2.0 build 2 [connected to 10.10.4.120 (GSSCP_IPO_10 (Server Edition(P)))] **********
 336128685mS SIP Rx: TCP 10.10.4.30:43844 -> 10.10.4.120:5060
                   OPTIONS sip:avaya.com SIP/2.0
                   From: <sip:avaya.com>;tag=1c1904606935
                   To: <sip:avaya.com>
                   CSeq: 1 OPTIONS
                   Call-ID: 07a0401e5c819c50fc33700dd0e04846
                   Contact: <sip:10.10.4.30:5060;transport=tcp>
                   Record-Route: <sip:10.10.4.30:5060;ipcs-line=2;lr;transport=tcp>
                   Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
                   Supported: replaces
                   User-Agent: M800B/v.7.20A.158.056
                   Max-Forwards: 69
                   Via: SIP/2.0/TCP 10.10.4.30:5060;branch=z9hG4bK-s1632-000939282561-1--s1632-
                   Accept: application/sdp, application/simple-message-summary, message/sipfrag
                   Content-Length: 0

 336128686mS Sip: Association found trunk: SIP Line (17)
 336128686mS Sip: Update SipTCPUser->trnk SIP Line (17)
 336128686mS Sip: SIPDialog f6e2cdd0 created, dialogs 1 txn_keys 1
 336128686mS Sip: (f6e2cdd0) SetUnIntTransactionCondition to UnInt_None
 336128686mS Sip: SipTCPUser 8430 has 1 dialog open (AttachDialogToSipTCPUser)
 336128686mS Sip: SIPDialog::ExtractResponseParamsFromViaHeader remote sent_by: 10.10.4.30:5060 trunk
 336128686mS Sip: SIPDialog::ExtractResponseParamsFromViaHeader remote sent by transport: SIP/2.0/TCP trunk
 336128686mS Sip: (f6e2cdd0) SendSIPResponse: OPTIONS code 200 SENT TO 10.10.4.30 43844
 336128686mS SIP Tx: TCP 10.10.4.120:5060 -> 10.10.4.30:43844
                   SIP/2.0 200 OK
                   Via: SIP/2.0/TCP 10.10.4.30:5060;branch=z9hG4bK-s1632-000939282561-1--s1632-
                   Record-Route: <sip:10.10.4.30:5060;ipcs-line=2;lr;transport=tcp>
                   From: <sip:avaya.com>;tag=1c1904606935
                   Call-ID: 07a0401e5c819c50fc33700dd0e04846
                   CSeq: 1 OPTIONS
                   Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
                   Supported: timer
                   Server: IP Office 10.1.0.2.0 build 2
                   To: <sip:avaya.com>;tag=895dd2b8d0f38743
                   Content-Type: application/sdp
                   Content-Length: 169

                   v=0
                   o=UserA 1712183164 1334060956 IN IP4 10.10.4.120
                   s=Session SDP
                   c=IN IP4 10.10.4.120
                   t=0 0
```

8.2. Avaya SBC

This section provides verification steps that may be performed with the Avaya SBC.

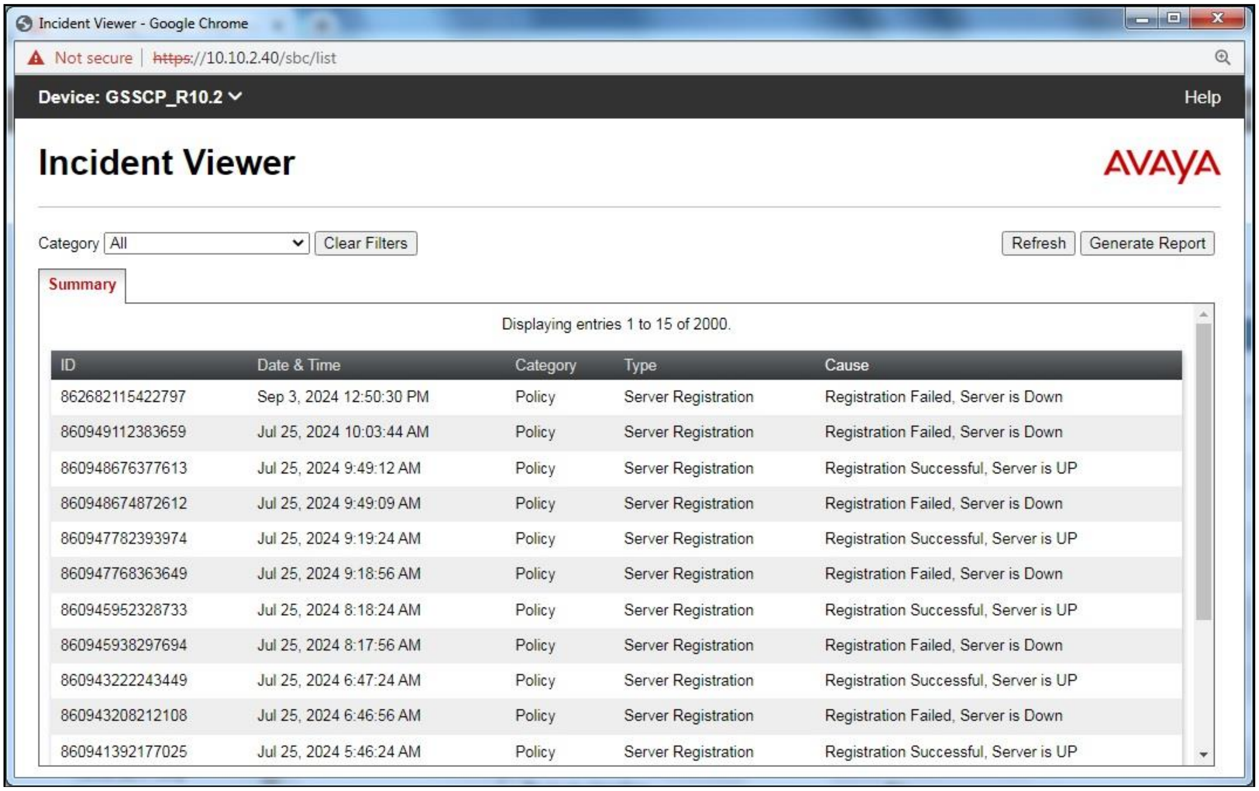
8.2.1. Incidents

The Incident Viewer can be accessed from the Avaya SBC dashboard as highlighted in the screen shot below.



Device Name	Management IP	Version	Status	
GSSCP_R10.2	10.10.2.40	10.2.0.1-89-24401	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures.



Incident Viewer

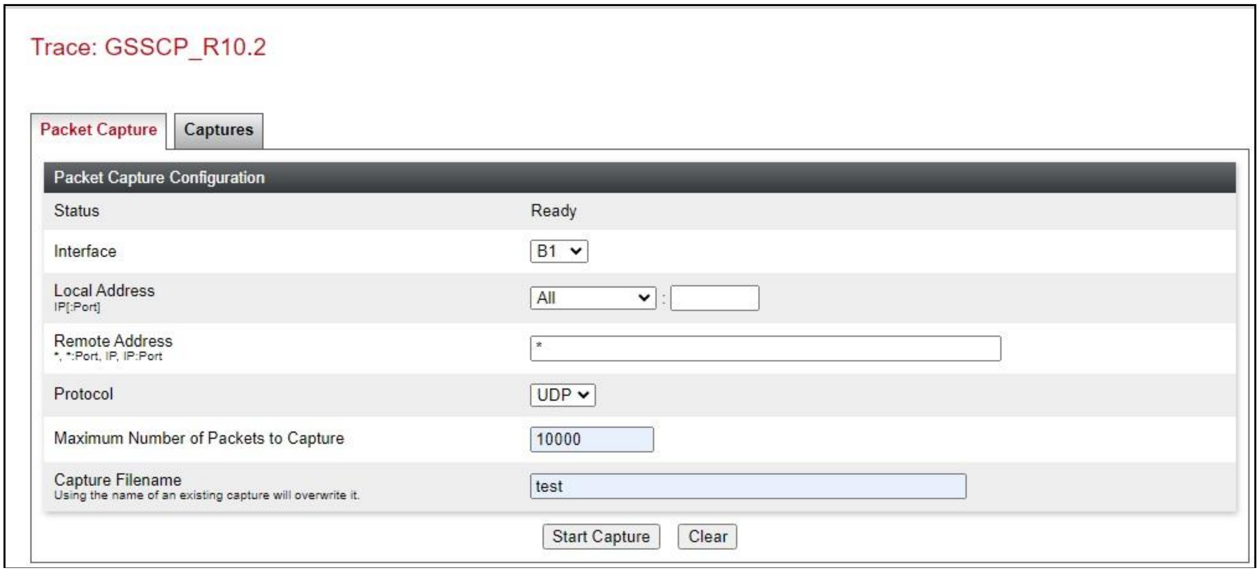
Displaying entries 1 to 15 of 2000.

ID	Date & Time	Category	Type	Cause
862682115422797	Sep 3, 2024 12:50:30 PM	Policy	Server Registration	Registration Failed, Server is Down
860949112383659	Jul 25, 2024 10:03:44 AM	Policy	Server Registration	Registration Failed, Server is Down
860948676377613	Jul 25, 2024 9:49:12 AM	Policy	Server Registration	Registration Successful, Server is UP
860948674872612	Jul 25, 2024 9:49:09 AM	Policy	Server Registration	Registration Failed, Server is Down
860947782393974	Jul 25, 2024 9:19:24 AM	Policy	Server Registration	Registration Successful, Server is UP
860947768363649	Jul 25, 2024 9:18:56 AM	Policy	Server Registration	Registration Failed, Server is Down
860945952328733	Jul 25, 2024 8:18:24 AM	Policy	Server Registration	Registration Successful, Server is UP
860945938297694	Jul 25, 2024 8:17:56 AM	Policy	Server Registration	Registration Failed, Server is Down
860943222243449	Jul 25, 2024 6:47:24 AM	Policy	Server Registration	Registration Successful, Server is UP
860943208212108	Jul 25, 2024 6:46:56 AM	Policy	Server Registration	Registration Failed, Server is Down
860941392177025	Jul 25, 2024 5:46:24 AM	Policy	Server Registration	Registration Successful, Server is UP

8.2.2. Trace Capture

To define the trace, navigate to **Device Specific Settings →Troubleshooting → Trace** in the menu on the left-hand side and select the **Packet Capture** tab.

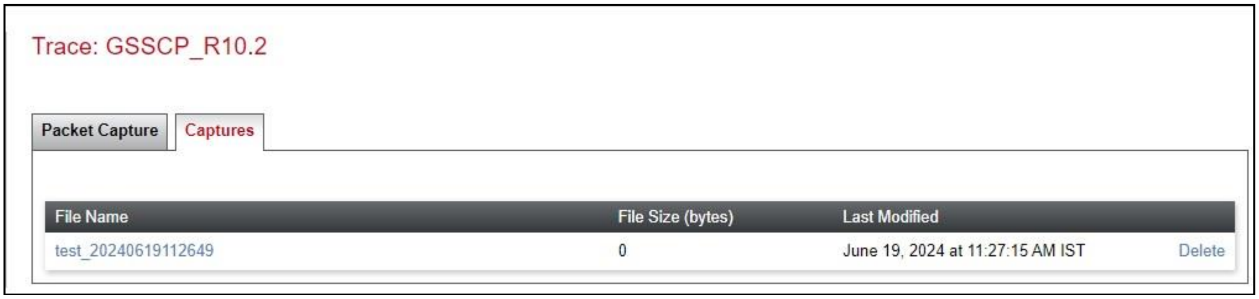
- Select the SIP Trunk interface from the **Interface** drop down menu.
- Select **All** from the **Local Address** drop down menu.
- Enter the IP address of the Service Provider's SBC in the **Remote Address** field or enter a * to capture all traffic.
- Specify the **Maximum Number of Packets to Capture**, 1000 is shown as an example.
- Specify the filename of the resultant .pcap file in the **Capture Filename** field.
- Click on **Start Capture**.



Trace: GSSCP_R10.2

Packet Capture Configuration	
Status	Ready
Interface	B1
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	UDP
Maximum Number of Packets to Capture	10000
Capture Filename Using the name of an existing capture will overwrite it.	test

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.



Trace: GSSCP_R10.2

File Name	File Size (bytes)	Last Modified	
test_20240619112649	0	June 19, 2024 at 11:27:15 AM IST	Delete

The trace is viewed as a standard .pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response in the form of a 200 OK will be seen from the Swisscom network.

9. Conclusion

These Application Notes demonstrated how IP Office Server Edition R12.0 and Avaya Session Border Controller R10.2 can be successfully combined with Swisscom Enterprise SIP Trunk Service as shown in **Figure 1**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and demonstrates Avaya IP Office with Avaya Session Border Controller can be configured to interoperate successfully with Swisscom Enterprise SIP Trunk Service. This solution provides IP Office and Avaya Session Border Controller users the ability to access the Public Switched Telephone Network (PSTN) via a SIP trunk with Swisscom Enterprise SIP Trunk Service thus eliminating the costs of analog or digital trunk connections previously required to access the PSTN. The service was successfully tested with a number of observations listed in **Section 2.2**.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

[1] *Deploying IP Office as Virtual Servers*, Release 12.0, Apr 2024.

[2] *Deploying IP Office Server Edition Servers*, Release 12.0, Apr 2024.

[3] *Deploying an IP500 V2 IP Office System*, Release 12.0, Apr 2024.

[4] *Administering Avaya IP Office with IP Office Web Manager*, Release 12.0, May 2024.

[5] *Administering Avaya IP Office with IP Office Manager*, Release 12.0, May 2024.

[6] *Using Avaya IP Office System Status*, Apr 2024.

[7] *Using IP Office System Monitor*, Apr 2024.

[8] *Administrating Voicemail Pro*, Release 12.0, May 2024.

[9] *Using Avaya Workplace Client for Windows*, Nov 2023.

[10] *IP Office SIP Phone Installation Notes,* Apr 2024.

[11] *Deploying Avaya Session Border Controller Release 10.2*, Apr 2024.

[12] *Upgrading Avaya Session Border Controller Release 10.2,* Mar 2024.

[13] *Administering Avaya Session Border Controller Release 10.2,* Apr 2024.

[14] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/

2024 Avaya LLC. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.